GOVERNMENT GAZETTE

OF THE

REPUBLIC OF NAMIBIA

N$8.00 WINDHOEK - 1 September 2023 No. 8200

CONTENTS

Page

General Notice

BANK OF NAMIBIA

No. 516 2023

CYBER SECURITY RULES: VIRTUAL ASSETS ACT, 2023

The Bank of Namibia designated as the Regulatory Authority in terms of section 5(1) of the Virtual Assets Act, 2023 (Act No. 10 of 2023) has in terms of section 51(1) of that Act made the Cyber Security Rules set out in the Schedule.

J. !GAWAXAB
GOVERNOR
BANK OF NAMIBIA

SCHEDULE

PART 1

DEFINITIONS AND SCOPE OF RULES

PART 2

GENERAL REGUIREMENTS

PART 3

BUSINESS CONTINUITY

PART 4

INSURANCE

PART 5

ENFORCEMENT

PART 6

SHORT TITLE

PART 7

EFFECTIVE DATE

PART 1

DEFINITIONS AND SCOPE OF RULES

Definitions

1. In these rules, a word or an expression to which a meaning has been given in the Virtual Assets Act, 2023(Act No. 10 of 2023) has that meaning, and –

"business continuity plan" means the business continuity plan created under rule 6;

"financial year" means the financial year referred to in section 21(1) of the Act;

"forks" mean changes to the software on which a blockchain protocol operates;

"the Act" means the Virtual Assets Act, 2023 (Act No. 10 of 2023).

Scope of rules

2. (1) These rules apply to persons issued with a licence under the Act to operate virtual asset service providers or as token issuers.

(2) These rules must be read together with the Act, regulations, rules, directives and guidelines issued under the Act as well as laws relating to money laundering and terrorism financing and proliferation activities and other applicable laws.

PART 2

GENERAL REGUIREMENTS

General requirements

3. (1) A licence holder must establish and maintain appropriate systems and controls for managing cybersecurity and operational risks that can arise from inadequacies or failures in the licence holder's processes and systems and this includes ensuring that there are the necessary resources in place to manage these risks.

(2) A licence holder must consider and ensure –

(a) the importance and complexity of processes and systems used in the end-to-end operating cycle for products and activities;

(b) that the licence holder's technology governance and risk assessment is capable of determining the necessary processes and controls that the licence holder must implement in order to adequately mitigate any risks identified, and the technology governance and risk assessment framework must include consideration of international standards and industry best practice codes;

(c) controls that help the licence holder to prevent system and process failures or identify systems and process failures to permit prompt rectification;

(d) whether the design and use of the licence holder's processes and systems allow the licence holder to comply adequately with the licence holders contractual obligations;

(e) the appropriateness of the licence holder's systems acquisition, development and maintenance activities, including the allocation of responsibilities between information technology development and operational areas, as well as its processes for embedding security requirements into systems;

(f) the allocation of responsibilities between business and technology areas;

(g) that the licence holder has arrangements for the continuity of operations in the event that a significant process or system becomes unavailable or is destroyed; and

(h) the importance of monitoring to quickly detect cyber incidents and periodically evaluate the effectiveness of systems and controls.

(3) A licence holder must consider the impact of any outsourcing arrangements, as well as the interoperability risks when dealing with software and systems provided by third parties, and as part of this, a licence holder must seek to identify any dependencies of its business and protect its clients against any cybersecurity and operational risk caused as a consequence of these dependencies.

(4) A licence holder must ensure that there is adequate oversight over its cybersecurity systems, and that there are clearly defined roles, responsibilities and accountability for staff or persons implementing, managing, and overseeing the effectiveness of the licence holder's cybersecurity strategy and framework.

(5) A licence holder must ensure the adequacy of its internal documentation of processes and systems, including how documentation is developed, maintained and distributed, in managing operational and cybersecurity risk.

(6) A licence holder must ensure that staff receive appropriate training in relation to cybersecurity.

(7) A licence holder must review his or her or its cybersecurity strategy and framework regularly, and at least annually, in response to changes in cyber risks generally as well as in response to any issues or weaknesses identified specific to the licence holder.

(8) A licence holder must annually submit to the Regulatory Authority the results of the review of licence holder's cybersecurity strategy and framework and operational resilience.

Systems and controls

4. (1) A licence holder must establish and maintain appropriate systems and controls to manage its cybersecurity and data risks and in doing so, a licence holder must have regard to –

(a) confidentiality, including the safe storage and transmission of data in accordance with clear protocols, and information must be accessible only to persons or systems with appropriate authority, which may require firewalls within a system, as well as entry restrictions;

(b) integrity, including safeguarding the accuracy and completeness of information and its processing;

(c) availability and authentication, including ensuring that only appropriately authorised persons or systems have access to the information when required and that their identity is verified by the licence holder;

(d) maintenance of systems and infrastructure, including ensuring proper code version control, implementation of updates, issue resolution, and externally carried out technology testing procedures; and

(e) procedures to address updates to technological infrastructure, as well as forks.

(2) A licence holder must ensure the adequacy of the systems and controls used to protect the processing and security of the licence holder's information, and must have regard to established security standards.

(3) A licence holder must obtain external testing and audits carried out by suitably qualified external experts, at least annually, and more frequently if appropriate given the nature and size of the licence holder's business.

PART 3

BUSINESS CONTINUITY

Unforeseen interruptions

5. (1) A licence holder must implement appropriate arrangements to maintain the continuity of its operations including load shedding incidents.

(2) A licence holder must act to reduce both the likelihood of a disruption, including by succession planning, systems resilience and dual processing, and the impact of a disruption, including by contingency arrangements and insurance.

(3) A licence holder must consider the likelihood and impact of a disruption to the continuity of its operations from unexpected events and this must include assessing the disruptions to which it is particularly susceptible and the likely timescale of those disruptions.

(4) The arrangements the licence holder has in place must be regularly updated and tested to ensure their effectiveness.

Business continuity plan

6. (1) A licence holder must document in his or her or its business continuity plan the strategy for maintaining continuity of his or her or its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy.

(2) A licence holder must establish –

(a) formal business continuity plans that outline arrangements to reduce the impact of a short, medium or long-term disruption, including –

(i) resource requirements such as people, systems and other assets, and arrangements for obtaining these resources;

(ii) the recovery priorities for the licence holder's operations; and

(iii) communication arrangements for internal and external concerned parties;

(b) escalation and invocation plans that outline the processes for implementing the business continuity plans, together with relevant contact information;

(c) processes to validate the integrity of information affected by the disruption; and

(d) processes to review and update the plans and processes referred to in paragraphs (a), (b) and (c) following changes to the licence holder's operations or risk profile, including changes identified through testing.

(3) The use of an alternative site for recovery of operations is common practice in business continuity management and a licence holder that uses an alternative site must assess the appropriateness of the site, particularly for location, speed of recovery and adequacy of resources.

(4) Where an alternative site for recovery operations is shared, a licence holder must evaluate the risk of multiple calls on shared resources and adjust the licence holder's plans accordingly.

(5) A licence holder must document his or her or its use of any alternative site in his or her or its business plan, and any changes in the alternative site used by the licence holder is considered to be a material change to the business continuity plan.

(6) A licence holder must review and test his or her or its business continuity plan annually to ensure that the licence holder is up to date, and this review must be completed within four months after the end of the financial year.

Geographic location

7. (1) In drafting the business continuity plan a licence holder must consider how operating processes and systems at separate geographic locations may alter a licence holder's risk profile, including by allowing alternative sites for the continuity of operations.

(2) A licence holder must document how the licence holder has considered the effect of any differences in processes and systems at each of the licence holder's locations, particularly if they are in different countries, having regard to –

(a) the business operating environment of each country, for example, the likelihood and impact of political disruptions or cultural differences on the provision of services;

(b) relevant local regulatory and other requirements regarding data protection and transfer;

(c) the extent to which local regulatory and other requirements may restrict the licence holder's ability to meet regulatory obligations in Namibia; and

(d) the timeliness of information flows to and from the licence holder's headquarter and whether the level of delegated authority and the risk management structures of the overseas operation are compatible with the licence holder's arrangements.

PART 4

INSURANCE

Use of insurance

8. (1) A licence holder may not assume that insurance alone can replace robust systems and controls, and must also consider nonmonetary impacts, such as the impact on the licence holder's reputation.

(2) When considering utilising insurance, a licence holder must consider –

(a) the time taken for the insurer to pay claims, including the potential time taken in disputing cover, and the licence holder's funding of operations whilst awaiting payment of claims;

(b) the financial strength of the insurer, which may determine its ability to pay claims, particularly where large or numerous small claims are made at the same time; and

(c) the effect of any limiting conditions and exclusion clauses that may restrict cover to a small or limited number of specific losses and may exclude larger or hard to quantify indirect losses, such as lost business or reputational costs.

PART 5

ENFORCEMENT

Enforcement

9. Where a licence holder or a person to whom these rules apply contravenes or fails to comply with a provision of these rules, the Regulatory Authority, may as it consider appropriate in the circumstance and in accordance with the Act, issue a directive, suspend or cancel a licence or amend a condition of a licence, or impose administrative sanctions or institute criminal proceedings in terms of the Act.

PART 6

SHORT TITLE

Short title

10. These rules may be cited as the Cyber Security Rules.

PART 7

EFFECTIVE DATE

Effective date

11. These rules become effective on the date of publication in the *Gazette.*