S.I. 71 of 2024

VIRTUAL ASSET SERVICE PROVIDERS ACT

(Act 12 of 2024)

Virtual Asset Service Providers (Cyber Security Requirements) Regulations, 2024

Arrangement of Regulations

Regulations

S.I. 71 of 2024

VIRTUAL ASSET SERVICE PROVIDERS ACT

(Act 12 of 2024)

Virtual Asset Service Providers (Cyber Security Requirements) Regulations, 2024

In exercise of the powers conferred by section 38(2)(f)(iv) of the Virtual Asset Service Providers Act, 2024, the Minister responsible for Finance, in consultation with the Authority makes the following Regulations —

Citation

1. These Regulations may be cited as the Virtual Asset Service Providers (Cyber Security Requirements) Regulations, 2024.

Interpretation

2. In these Regulations —

"business continuity plan" means the plan required to be established under regulation 11;

"cyber security" means an approach or series of steps to prevent or manage the risk of damage to, unauthorized use of, exploitation of and, as needed, to restore electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems;

"cyber security event" means any act or attempt, successful or unsuccessful, to gain unauthorized access to disrupt, or misuse the electronic systems or information stored on such systems;

"cyber security risk" means the risk of financial loss, operational disruption or damage from the failure of the digital technologies

employed for informational and/or operational functions introduced to an information system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system;

"forks" means changes to the software on which a blockchain protocol operates.

Application

3. These Regulations shall apply to all licensees.

Cyber security strategy

4.(1) A licensee shall have in place a cyber security strategy for the establishment and maintenance of appropriate systems and controls for managing cyber security and operational risks that can arise from inadequacies or failures in its processes and systems.

(2) Further to subregulation (1), the licensee shall also include appropriate systems and processes with or from third-party suppliers, agents and intermediaries.

(3) The requirements under subregulations (1) and (2) shall include the necessary resources to —

(a) manage cyber security risks;

(b) identify, respond and prevent a cyber security event;

(c) limit the damages that may arise from a cyber security risk.

(4) A licensee shall —

(a) implement controls to prevent system and process failures or in the event of such a failure, to identify them and undertake the necessary steps for prompt rectification;

(b) ensure that the design and use of its processes and systems allow it to comply with its contractual obligations with its clients, suppliers and its legal obligations;

(c) ensure the appropriateness of its system's acquisition, development and maintenance activities, including the allocation of responsibilities between IT development and operational areas, as well as its processes for embedding security requirements into systems;

(d) ensure that its arrangements for the continuity of operations in the event that a significant process or system becomes unavailable or is destroyed; and

(e) ensure adequate monitoring mechanisms are in place to quickly detect cyber incidents and periodically evaluate the effectiveness of systems and controls.

(5) A licensee shall consider the impact of any outsourcing arrangements, as well as the interoperability risks when dealing with software and systems provided by third parties.

(6) A licensee shall ensure that there is adequate senior management oversight over its cyber security systems with clearly defined roles, responsibilities and accountability for staff implementing, managing and overseeing the effectiveness of the licensee's cyber security strategy and policy.

(7) A licensee shall ensure that the documentation of its internal processes and systems is maintained and distributed in managing operational and cyber security risk.

(8) A licensee shall ensure that all staff receive appropriate training in relation to cyber security on a periodic basis.

(9) A licensee shall review its cyber security strategy and policy regularly, and at least annually, in response to changes in cyber security

risks, as well as in response to a cyber security event or to any issues or weaknesses identified specific to the licensee operation.

(10) Further to subregulation (9), the licensee shall submit the results of its review of the cyber security strategy and policy, and any remedial actions needed, to its board of directors as soon as practicable and, in any event, no later than one month after the date on which the review was approved by its board of directors to the Authority.

(11) Where a person acts in contravention of this regulation, the Authority shall take such enforcement action as it deems necessary under the Act, and may impose an administrative penalty of SCR4,000,000 and an additional SCR50,000 for each day or part of each day, not exceeding twenty days, for which the contravention continues.

Systems and controls

5.(1) In maintaining appropriate systems and controls under regulations 4(1) and 4(2), a licensee shall have regards to —

(a) confidentiality, including the safe storage of information and transmission of data in accordance with clear protocols, which may require firewalls within a system, as well as entry restrictions and compliance with relevant data protection laws;

(b) accessibility of the system to authorized persons, employees of the licensee and as the case maybe, to authorized employees of the Authority;

(c) integrity, including safeguarding the accuracy and completeness of information and data through its system and control;

(d) maintenance of systems and infrastructure, including proper code version control, implementation of updates and resolution; and

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

(2) A licensee shall ensure the adequacy of the systems and controls used to protect the processing and security of its information through established security standards.

(3) The systems and control of a licensee shall include, without limitation, the following audit functions —

(a) penetration testing of its systems and vulnerability assessment of those systems conducted on a bi-annual basis during the first year of licensing and at least once a year for subsequent years;

(b) audit trail systems that —

(i) track and maintain information and data that allows for the complete and accurate reconstruction of all financial transactions and accounting;

(ii) protect the integrity of data stored and maintained as a part of the audit trail from alteration or tampering;

(iii) protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;

(iv) log system events, including but not limited to access and alterations made to the audit trail systems and cyber security events;

(v) maintain records produced as part of the audit trail; and

(vi) the effectiveness of the safe keeping, storage and accessibility of the virtual assets being kept by the licensee.

(4) Subject to the approval of the Authority, a licensee shall appoint a qualified independent party to audit its systems and control, as and when may be required by the Authority, and provide a written opinion to the Authority that the licensee's program and controls are suitably designed and operating effectively to meet the licensee's obligations under these Regulations and any applicable regulations or code issued by the Authority under this Act.

(5) Further to subregulation (4), in making an appointment, a licensee shall consider and state in the resolution making the appointment whether the independent party conducting the audit, as the case may be, —

(a) holds the required qualifications and competence, has proven experience and adequate resources to perform the appointee's functions; and

(b) is independent of the licensee in that the appointee or, in the case of a firm, any of its partners has no relationship with, or interest in, the licensee, any of its group of companies, nor has any connection with any director or substantial shareholder of the licensee that could reasonably be perceived as materially affecting the exercise by the appointee of an independent mind and judgement in the performance of the appointee's duties.

(6) Where a person acts in contravention of subregulations (3) and (4), the Authority shall take such enforcement action as it deems necessary under the Act, and may impose an administrative penalty of SCR2,000,000 and an additional SCR50,000 for each day or part of each day, not exceeding thirty days, for which the contravention continues.

Unforeseen interruptions

6.(1) A licensee shall implement appropriate and effective arrangements to maintain the continuity of its operations in order to —

(a) reduce both the likelihood of a cyber security event; and

(b) mitigate the potential impact of a cyber security event on the licensee's operations.

(2) A licensee shall assess the likelihood and impact of a cyber security risk to the continuity of its operations arising from cyber security events and apply commensurate measures to minimize their occurrence.

Reporting of cyber security risk

7.(1) Where the licensee discovers a cyber security risk as a result of a cyber security event, it shall notify the Authority of any attempt within 24 hours.

(2) Further to subsection (1), for any successful attempt, the licensee shall provide a report within 5 working days on the whether the cyber security event —

(a) affects or has affected the services or network and information systems that support critical or important functions of the licensee;

(b) affects or has affected services for which the licensee has been authorized to provide; and

(c) constitutes or has constituted a malicious and unauthorized access to the network and information systems of the licensee.

(3) The report under subsection (2) shall also include the remedial actions to mitigate cyber security risk and prevent future cyber security event.

Cyber security report

8.(1) For the purpose of section 22(2) of the Act, a cyber security report shall be duly prepared by the fit and proper person responsible for information security, containing —

(a) the availability, functionality and integrity of the licensee's electronic systems;

(b) any identified cyber risk arising from any virtual asset service carried on or to be carried on, by the licensee; and

(c) the cyber security program implemented and proposals for steps for the redress of any inadequacies identified.

(2) Where a person acts in contravention of this regulation, the Authority shall take such enforcement action as it deems necessary under the Act and may impose an administrative penalty of SCR 500,000.

Group and related entities

9. In cases where a licensee forms part of a group, the Authority may consider the cyber security strategy and policy of the parent company, provided that same extends and encapsulated the operationalities of the licensee.

Data Protection

10. Licensees shall demonstrate that data protection is part of the cyber security strategy and policy taking into consideration the provisions of the Data Protection Act.

Business continuity plan

11.(1) A licensee shall have in place a formalized business continuity plan, as approved by its board of directors, and address its strategy for maintaining continuity of its operations, its plans for communicating and regularly testing the adequacy and effectiveness of this plan.

(2) The business continuity plan shall outline arrangements to reduce the impact of short, medium or long-term disruption, including —

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

(b) the recovery priorities for the licensee' operations; and

(c) communication arrangements for internal and external concerned parties

(3) A licensee shall review and test its business continuity plan at least every two years to ensure that it is up-to-date.

(4) A licensee shall make available its business continuity plan and/or its report depicting the results of its business continuity testing to the Authority, upon request, and within such time as may be indicated.

(5) Where a person acts in contravention of this regulation, the Authority shall take such enforcement action as it deems necessary under the Act, and may impose an administrative penalty of SCR 500,000 and an additional SCR50,000 for each day or part of each day, not exceeding thirty days, for which the contravention continues.

MADE this 5th day of September, 2024.

NAADIR HASSAN
MINISTER FOR FINANCE,
NATIONAL PLANNING AND TRADE