THE VIRTUAL ASSET AND INITIAL TOKEN OFFERINGS SERVICES ACT

FSC Rules made by the Financial Services Commission under section 52 of the Virtual Asset and Initial Token Offerings Services Act

PART I – GENERAL PROVISIONS

1. Citation

These rules may be cited as the Virtual Assets and Initial Token Offerings Services (Cybersecurity) Rules.

2. Interpretation

“Act” means the Virtual Asset and Initial Token Offerings Services Act ;

“applicable Acts” has the same meaning as in the Act;

"business continuity plan” means the business continuity plan created under Part III of these Rules;

“Commission” has the same meaning as in the Act;

“financial year” has the same meaning as in section 22 of the Act;

“forks” mean changes to the software on which a blockchain protocol operates.

“FSC Rules” has the same meaning as in the Act;

“person” has the same meaning as in the Act;

“relevant Acts” has the same meaning as in the Financial Services Act;

“virtual asset service provider” has the same meaning as in the Act.

3. Scope

(1) These rules shall apply to all virtual asset service providers that carry out business in or from Mauritius.
(2) These rules shall be read in conjunction with the Act, applicable Acts, relevant Acts and guidelines which the Commission may issue from time to time.

PART II – GENERAL REQUIREMENTS

4. The general requirements

(1) A virtual asset service provider should establish and maintain appropriate systems and controls for managing cybersecurity and operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third party suppliers, agents and others). This includes ensuring that there are the necessary resources in place to manage these risks.
(2) A virtual asset service provider shall consider and ensure:

(a) the importance and complexity of processes and systems used in the end-to-end operating cycle for products and activities (for example, the level of integration of systems);
(b) controls that shall help it to prevent system and process failures or identify them to permit prompt rectification;
(c) whether the design and use of its processes and systems allow it to comply adequately with its contractual obligations and the FSC Rules;
(d) the appropriateness of its systems 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);
(e) the allocation of responsibilities between business and technology areas;
(f) its arrangements for the continuity of operations in the event that a significant process or system becomes unavailable or is destroyed; and
(g) the importance of monitoring to quickly detect cyber incidents and periodically evaluate the effectiveness of systems and controls.

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

(4) A virtual asset service provider must ensure that there is adequate senior management oversight over its cybersecurity systems, and that there are clearly defined roles, responsibilities and accountability for personnel implementing, managing, and overseeing the effectiveness of the virtual asset service provider's cybersecurity strategy and framework.

(5) A virtual asset service provider should 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 virtual asset service provider should ensure that all staff receive appropriate training in relation to cybersecurity.

(7) A virtual asset service provider should review 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 virtual asset service provider.

(8) A virtual asset service provider should submit the results of its review of its cybersecurity strategy and framework and operational resilience to the Commission on an annual basis.

5. Systems and controls

(1) A virtual asset service provider should establish and maintain appropriate systems and controls to manage its cybersecurity and data risks. In doing so, a virtual asset service provider should have regard to:
(a) confidentiality, including the safe storage and transmission of data in accordance with clear protocols. Information should 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;
(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 virtual asset service provider should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards.

(3) A virtual asset service provider should 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 its business.

PART III – BUSINESS CONTINUITY

6. Unforeseen interruptions

(1) A virtual asset service provider should implement appropriate arrangements to maintain the continuity of its operations. A virtual asset service provider should 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).

(2) A virtual asset service provider should consider the likelihood and impact of a disruption to the continuity of its operations from unexpected events. This should include assessing the disruptions to which it is particularly susceptible (and the likely timescale of those disruptions).

(3) The arrangements the virtual asset service provider has in place should be regularly updated and tested to ensure their effectiveness.

7. Business continuity plan

(1) A virtual asset service provider should document in its business continuity plan its strategy for maintaining continuity of its operations, and its plans for communicating and regularly testing the adequacy and effectiveness of this strategy. A virtual asset service provider should 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 virtual asset service provider's operations; and
iii. communication arrangements for internal and external concerned parties (including the Commission, clients and the press);
(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 (a) to (c) following changes to the virtual asset service provider's operations or risk profile (including changes identified through testing).

(2) The use of an alternative site for recovery of operations is common practice in business continuity management. A virtual asset service provider that uses an alternative site should assess the appropriateness of the site, particularly for location, speed of recovery and adequacy of resources. Where a site is shared, a virtual asset service provider should evaluate the risk of multiple calls on shared resources and adjust its plans accordingly.

(3) A virtual asset service provider should document its use of any alternative site in its business plan, and any changes in the alternative site used by the virtual asset service provider shall be deemed a material change to the business continuity plan for the purpose of rule 4 of the Virtual Asset and Initial Token Offerings Services (Statutory Returns) Rules.

(4) A virtual asset service provider should review and test its business continuity plan annually to ensure that it is up to date, and this review should be completed within 4 months after the close of the financial year.

8. Geographic location

(1) In drafting the business continuity plan a virtual asset service provider should consider how operating processes and systems at separate geographic locations may alter a virtual asset service provider's risk profile (including by allowing alternative sites for the continuity of operations). A virtual asset service provider should document how it has considered the effect of any differences in processes and systems at each of its 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 its ability to meet regulatory obligations in Mauritius; and

(d) the timeliness of information flows to and from its headquarter and whether the level of delegated authority and the risk management structures of the overseas operation are compatible with the virtual asset service provider’s arrangements.

PART IV – INSURANCE

9. Use of insurance

(1) A virtual asset service provider should not assume that insurance alone can replace robust systems and controls. A virtual asset service provider should also consider non-monetary impacts, such as the impact on the virtual asset service provider's reputation.

(2) When considering utilising insurance, a virtual asset service provider should consider:

(e) the time taken for the insurer to pay claims (including the potential time taken in disputing cover) and the virtual asset service provider's funding of operations whilst awaiting payment of claims;

(f) 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

(g) 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).

10. Commencement

These rules shall come into operation on [**DATE**].

Made by the Financial Services Commission on [**DATE**].