Government Notice No. 44 of 2019

FINANCIAL SERVICES ACT

FSC Rules made by the Financial Services Commission under section 93 of the Financial Services Act

1. Citation

These rules may be cited as the Financial Services (Custodian services (digital asset)) Rules 2019.

2. Interpretation

In these rules –

"Act" means the Financial Services Act;

"alphanumeric phrase" means a list of words from a specific word set which are used to create a mnemonic containing all required information to use a key or apply a signature;

"air gap machine" means a computer specifically designed so that –

(a) it is not connected to the internet; and

(b) it operates without microphone, network interface card, wired network connectivity and Bluetooth;

"blockchain" means a type of distributed ledger technology which is a way of recording and sharing data across multiple data ledgers, with each individual ledger having the exact data records and are collectively maintained and controlled by a distributed network of computer servers referred to as nodes;

"cold storage" means a method of storing digital asset or information whereby the device used for storage is not connected to the internet;

"CIS manager" shall have the same meaning as in the Securities Act;

"core functions" means functions related to operational and governance protocols, safekeeping of digital asset and transaction management;

"custodian" means the entity entrusted with the custody of digital asset;

"custody" means the safekeeping of digital asset being held or transacted;

"digital asset" –

(a) means any token, in electronic or binary form, which is representative of either the holder's access rights to a service or ownership of an asset;

(b) includes a digital representation of value which –

(i) is used as a medium of exchange, unit of account, or store of value but which is not a legal tender, even if it is denominated in legal tender;

(ii) represents assets such as debt or equity; or

(iii) provides access to a blockchain-based application, service or product;

(c) excludes –

(i) any transaction in which a business, as part of an affinity or reward programme, grants value which cannot be exchanged for legal tender, bank credit or any digital asset; or

(ii) a digital representation of value issued for use within an online gaming platform.

"digital asset-agnostic" means the ability of the systems and procedures of the custodian to operate properly irrespective of the type of digital asset kept in custody;

"entropy" means unpredictability or randomness within the source code which is used to generate a cryptographic seed which ensures that a seed cannot be simply recreated;

"hot storage" means a method of storing digital asset or information whereby the device used for storage is connected to the internet;

"key" means a cryptographic key which is used by a cryptographic algorithm to transform plain text into encrypted form or vice versa;

"mnemonic" means the use of encoding, character or letter patterns or imagery as technique to encode information in a manner which enables efficient storage and retrieval;

"M-of-N multi-signature" means the requirement for a minimum number of signatures (M) out of the total number of available signatures (N) in order for a transaction to be initiated for a wallet;

"network interface card" means a hardware component which allows a computer to exchange data with a network;

"operational and governance protocols" means policies, protocols and operational risk management programme including fraud prevention in relation to the custody of digital asset;

"safekeeping of digital asset" means the contractual obligation according to which a custodian is required to secure and preserve digital asset being held in custody through the generation and

securing of seeds and keys as well as management of addresses and wallets relating to digital asset including recovery processes for seeds and keys which have either been corrupted or otherwise compromised;

"securities" shall have the same meaning as in the Securities Act;

"seed" means an alphanumeric phrase generated through the process of entropy;

"self-managed scheme" shall have the same meaning as in the Securities (Collective Investment Schemes and Closed-end Funds) Regulations 2008;

"signatory" means an individual providing one of the signatures in an M-of-N multi-signature transacting method;

"signature" means an authorization protected by cryptography which is applied by a designated signatory to initiate a transaction;

"transaction" means an exchange or operation specific to a digital asset being held in custody;

"transaction management" means procedures for the facilitation of incoming and outgoing transactions in relation to a digital asset being held in custody to ensure that appropriate internal controls are applied prior to any transactions being authorised;

"transaction timestamp" means a sequence of characters or encoded data enabling the identification of the occurrence of a particular transaction including the precise date and time at which the transaction occurred;

"transaction type" means the classification of a transaction according to its specific purpose and includes deposit and withdrawal;

"wallet" means a software application or other mechanism or medium used for holding, storing and transferring digital asset;

"wired network connectivity" means the capacity for a computer to connect to a network through the use of cables.

3. Scope of the rules

(1) These rules shall apply to any person carrying out custodian services for digital asset.

(2) These rules shall be read in conjunction with the relevant Acts and any guidelines which the Commission may issue from time to time.

4. Application for a licence

(1) No person shall carry out custody services for digital asset in Mauritius without a Custodian services (digital asset) licence issued by the Commission.

(2) An application for a Custodian services (digital asset) licence shall be made in accordance with Part IV of the Act.

(3) The objects of a custodian under these rules shall be limited to the safe-keeping of digital asset and operations arising directly from it.

5. Letter of intent to be issued

(1) Subject to the Commission being satisfied that the application meets the requirements of the Act and these rules, it may issue a letter of intent to the applicant.

(2) The applicant shall, within 6 months from the date of the letter of intent or such other period as may be approved by the Commission, demonstrate that it has in place, the required resources, infrastructure and staffing to commence business as set out in its application.

(3) A letter of intent issued under paragraph (1) –

(a) may be revoked at any time by the Commission;

(b) shall not imply or be construed in any way as a promise or an undertaking by the Commission, nor import any obligation on the part of the Commission, to grant a Custodian services (digital asset) licence or otherwise determine an application.

(4) Where the Commission is satisfied that the applicant meets the requirements of paragraph (2), it may grant the Custodian services (digital asset) licence.

(5) A custodian shall commence business within 6 months from the date on which the Custodian services (digital asset) licence was granted.

(6) When assessing whether a custodian has commenced business, the Commission may have regard to –

(a) the number of clients of the custodian;

(b) the value of digital asset under its custody;

(c) the number of transactions undertaken by the custodian; and

(d) such other information as it may deem appropriate.

6. Operations in Mauritius

(1) A custodian shall, at all times, have –

(a) an office in Mauritius from which it shall perform its core functions; and

(b) a representative in Mauritius who shall be an officer of sufficiently senior status and knowledgeable in the operations of the custodian.

(2) The representative shall be responsible for providing such services as the custodian may require in Mauritius, including –

(a) filing with the Commission such document as may be required under the relevant Acts and any other enactment;

(b) acting as liaison with the Commission for any correspondence, notice or summons; and

(c) maintaining records of the custodian, including board minutes and resolutions, transaction records and such other documents as the Commission may require.

7. Governance

A custodian shall, at all times, –

(a) ensure that its governance structure provides effective oversight of its activities, taking into consideration the nature, scale and complexity of its business;

(b) have adequate internal controls and adopt strategies, policies, processes and procedures in accordance with principles of sound corporate governance and risk management;

(c) maintain its registered office and place of business in Mauritius; and

(d) be managed by a board of directors composed of a minimum of 3 directors, of which at least -

(i) 30 per cent shall be independent directors; and

(ii) one shall be resident in Mauritius.

8. Adequacy and competency of staff

(1) A custodian shall be required to -

(a) have a suitable number of staff with the appropriate competence, experience and proficiency to properly perform its core functions;

(b) subject all staff involved in core functions, whether automated or manually executed, to vetting and clearance through appropriate background screening or other appropriate tests in accordance with best industry standards prior to recruitment and thereafter on a recurrent basis;

(c) have properly defined and documented duties and responsibilities for all staff performing core functions; and

(d) ensure that staff are provided with appropriate training on a regular basis for their respective duties and responsibilities.

(2) A custodian shall keep appropriate records to demonstrate its compliance with paragraph (1) and such records must be made available to the Commission upon request.

9. Disaster Recovery and Business Continuity

(1) A custodian shall have a redundancy system to ensure the continuity of its operations in the event that -

(a) the equipment and software used to perform core functions are not available from the main supplier; and

(b) the primary staff assigned to perform a non-automated core function is unavailable.

(2) A custodian shall maintain appropriate disaster recovery facilities, with geographic segregation and equivalent security installations as its primary place of business in the event that such primary place of business becomes inoperative, to ensure business continuity and client asset protection.

10. Minimum Capital Requirement

A custodian shall, at all times, have and maintain a minimum stated unimpaired capital which is the higher of –

(a) 35 million rupees or an equivalent amount; or

(b) an amount representing 6 months' operating expenses as reported in the audited financial statements submitted to the Commission.

11. Management of operational risks

(1) A custodian shall set up and maintain, at all times, a risk management framework to enable it to effectively develop and implement strategies, policies, procedures and controls to manage its operational risks.

(2) A custodian shall have a comprehensively documented operational risk management programme (ORMP) which shall –

(a) include all current industry risks;

(b) be audited on an on-going basis to cater for emerging risks to its business; and

(c) be communicated to all relevant staff.

(3) The ORMP shall include, at a minimum –

(a) strategies developed to identify, assess, monitor and mitigate operational risks;

(b) policies and protocols relating to operational risk management and controls;

(c) methodology to assess operational risks; and

(d) operational risk reporting system.

(4) For any use of automation to perform core and other operational functions, the custodian shall include in the ORMP, scenarios to be followed in the event that the automation fails.

(5) The board of the custodian shall be ultimately responsible for the ORMP and its implementation.

12. Infrastructure for continuous operations

(1) A custodian shall have appropriate infrastructure in place to ensure that its core functions are fully operational at all times.

(2) A custodian shall have appropriate systems and procedures to ensure that it operates efficiently and completes transactions in a timely manner in accordance with industry best practices and standards.

13. Custody processes and systems testing

(1) A custodian shall cause its custody systems and processes to be tested on a quarterly basis.

(2) The testing of the custody systems and processes shall include –

(a) penetration testing and vulnerability scans;

(b) wallet integrity audits;

(c) key and seed generation procedures;

(d) complete transaction audit to ensure compliance with protocols;

(e) suspicious transaction handling; and

(f) migration of storage devices including cold to hot storage and vice versa.

(3) The systems and processes shall be tested in line with best industry standards and practices internally by the custodian and by an independent third party appointed by the custodian.

(4) Records of such tests shall be maintained by the custodian and made available to the Commission for inspection, upon request.

14. Incident Reporting

(1) A custodian shall have in place appropriate protocols to ensure that any incident resulting in an interruption of its operations is logged and documented with details including –

(a) the cause of the incident;

(b) the impact on the operations;

(c) the method used to resolve the incident; and

(d) the duration of the interruption.

(2) A custodian shall prepare a report for every incident referred to in paragraph (1) and submit that report to its board of directors for informational purposes.

(3) Where appropriate, the custodian shall use each incident report referred to in paragraph (2), to update its custody systems.

15. External audit of policies and procedures

(1) A custodian shall appoint an external independent third party to undertake an audit of all its systems, policies and processes regularly and in any case at least once every year.

(2) A custodian shall ensure that the external independent third party which it has appointed has the appropriate competence in line with best industry standards and practices to undertake the audit referred to in paragraph (1).

(3) A custodian shall notify the Commission of the external independent third party appointed under paragraph (2) and shall submit –

(a) full particulars of the external independent third party; and

(b) an undertaking that the external independent third party has the appropriate competence to undertake the audit.

(4) The Commission may object to the appointment of the external independent third party where it considers that the external independent third party does not have the competence to undertake the audit.

(5) A custodian shall submit the report of the external independent third party for the consideration of its board and shall address any shortcomings identified in the report.

(6) Records of such audits and any remedial actions implemented shall be maintained by the custodian and made available to the Commission for inspection, upon request.

16. Outsourcing

(1) Except with the prior approval of the Commission, a custodian shall not delegate or outsource any of its core functions.

(2) A custodian shall have a documented policy regarding the outsourcing of its non-core functions.

(3) When delegating or outsourcing a non-core function, the custodian shall conduct appropriate due diligence to ensure that the delegate is fit and proper and has the capacity to fulfil the delegated function in accordance with these rules.

(4) A custodian shall not be discharged from its responsibilities upon any delegation or outsourcing arrangement and shall, at all times, ensure compliance with the requirements of the relevant Acts.

(5) A custodian shall ensure that all books and records relating to the function delegated or outsourced are made available for inspection by the Commission.

17. Custody agreements

(1) An agreement for custody and safe-keeping of digital asset shall provide for –

(a) the services to be provided to the client under the custody agreement and the related fees;

(b) requirements as regards the location of assets;

(c) the method of holding assets; and

(d) the standard of care to be exercised by the custodian and its responsibility for loss of the digital asset.

(2) In case the digital asset is being held for a collective investment scheme, the custody agreement shall provide –

(a) for the custodian agreeing to the constitutive documents, prospectus or offering document of the collective investment scheme;

(b) that only the CIS manager or the self-managed scheme may give instructions to the custodian; and

(c) for the custodian to forthwith submit a report to the Commission, and a copy thereof to the CIS manager and the scheme, in relation to any failure of the CIS manager or the scheme to meet the requirements applicable to the conduct of its business activities.

(3) No agreement between a CIS manager or a collective investment scheme with a custodian shall provide for the creation of any encumbrance on the assets of the collective investment scheme except in relation to a claim for payment of the fees and expenses of the custodian for acting in that capacity.

18. Communication with clients

(1) A custodian shall have in place such procedures as may be required to ensure that –

(a) each client is provided with an original of the signed agreement regarding the custody of digital asset within 30 days from the date on which the agreement is signed; and

(b) each client is promptly informed of any action which is likely to impact on any provisions of the agreement and on digital asset being held in custody.

(2) In the event that such disclosures are being made to a client through an internet-based service, a custodian shall have in place a multi-factor authentication system in line with best industry practices

19. Key and Seed Generation

(1) A custodian shall have safeguards embedded in the seed creation and key generation processes to ensure that seeds and keys are resistant to speculation or collusion.

(2) A custodian shall adhere to best industry standards and practices in terms of entropy for the generation of asymmetric private-public key combinations to ensure unpredictability and randomness.

(3) A custodian shall include a mnemonic back-up phrase which is generated as part of the seed to be used to regenerate the seed if required.

(4) A custodian shall have at least 3 staff members involved in the process of generating entropy during seed creation and have appropriate measures to ensure that no single staff has information on the entirety of the seed or the mnemonic phrase.

(5) A custodian shall have adequate procedures to ensure that staff involved in seed creation are not involved in systems and processes for the initiation of transactions.

(6) A custodian shall ensure that seed creation and key generation are carried out on an air gap machine or such other hardware security modules, in accordance with industry best practices, located in a secured physical space which is resilient against physical or network-based malicious attacks.

(7) A custodian shall ensure that each seed is stored on an encrypted, password-secured device.

(8) A custodian shall cause all data post seed creation and key generation, including entropy procedures, seeds, private keys, or any other sensitive wallet information created during the seed creation and key generation, to be securely deleted or destroyed.

20. Key and Seed Storage

(1) A custodian shall ensure that any key and seed which are not in use are stored in an encrypted form on a password-secured device.

(2) A custodian shall have appropriate systems and processes to ensure that-

(a) the required number of keys to initiate a transaction are not stored together, whether online or at a single physical location; and

(b) no transaction can be initiated using solely keys stored online or at a physical location.

(3) A custodian shall –

(a) cause the mnemonic back-up phrase to be broken into at least 3 distinct parts with each part being stored separately in distinct tamper-proof containers stored in different physically secure locations; and

(b) ensure that a sufficient number of parts of the mnemonic back-up phrase required to regenerate the seed, are not stored in a single location.

(4) A custodian shall ensure that storage of back-up seeds is off-site from the premises where transactions are managed and custody operations are conducted.

(5) The off-site storage mentioned in paragraph (4) shall be operated by a third party and shall be equipped with safe deposit boxes enabling dual key access and security features including continuous video monitoring and protection against forcible attacks, flood, fire, cyclone and other climatic conditions.

(6) A custodian shall ensure that access to off-site back-up seed storage is restricted solely to authorised staff whose identity must be verified and confirmed by the third party through multifactor identity verification and audit consistent with industry best practices prior to granting access.

(7) A custodian shall cause an internal audit of its systems and processes relating to back-up seeds to be conducted, at a minimum, on a quarterly basis to assess any unauthorised access.

(8) The results of the audit mentioned in paragraph (7), must be properly recorded with details of any incidents observed as well as any remedial actions taken, if any, and shall be provided to the Commission upon request.

21. Access by Staff to Keys, Seeds and related information

(1) A custodian shall restrict access to keys, seeds and other information relating to digital asset being held in custody solely to authorised staff on a demonstrated business needs basis.

(2) An updated list of authorised staff having such access shall be maintained by the custodian along with clearly defined procedures to enable or revoke access rights.

(3) Access rights to keys, seeds and related information must be adequately logged to evidence access rights management.

22. Impaired Key

(1) A custodian shall have systems and procedures to be implemented in the event that it has reasonable grounds to believe that a key, seed or a part thereof has been compromised, including for an investigation to be conducted and appropriate remedial actions to be taken.

(2) The investigation findings including remedial actions taken, if any, shall be provided to the Commission upon request.

23. Uninterrupted Access

A custodian shall, subject to the custody agreement, provide its clients with uninterrupted access to their respective digital asset under its custody if –

(a) it is no longer able to abide by the custody agreement; or

(b) it ceases to operate; or

(c) it is requested to transfer the digital asset in accordance with the instructions of the client or such other mutually agreeable arrangements.

24. Segregation of client assets

(1) A custodian shall have adequate procedures to ensure that digital asset belonging to different clients are not pooled or not kept together at a single address or in a common wallet.

(2) A custodian shall ensure that an address or wallet is assigned to a single client and that the digital asset belonging to that client is kept in the assigned address or wallet.

25. Security infrastructure for on-site cold storage of digital assets

(1) A custodian shall have in place a secured physical infrastructure, including but not be limited to guarded access to the facilities with restricted admittance to authorised staff only, vault storage with dual key requirements and uninterrupted closed-circuit television system.

(2) Access procedures will have to be adequately documented and shall be made available to the Commission upon request.

26. Storage strategy for digital assets

(1) A custodian shall have in place a strategy, in accordance with best industry standards and practices, for selecting the appropriate storage for a digital asset to be kept in custody considering factors including -

(a) the volume of transactions relating to the digital asset;

(b) the speed at which those transactions are to be executed; and

(c) risk appetite of the client.

27. Procedures for security breaches

(1) A custodian shall have procedures in place to protect the digital asset being held in custody in the event, or suspicion of, a security breach including hacking, attack, theft or any situation whereby a digital asset being kept in custody has been compromised.

(2) A custodian shall promptly notify the client of any security incident relating to digital asset under custody.

(3) A custodian shall have the procedures mentioned in paragraph (1) audited on a yearly basis by an external independent third party.

28. Revocation of a signatory's access key to a back-up seed

(1) A custodian shall have appropriate systems and procedures for the immediate revocation of the key held by a signatory to prevent the signatory from accessing or recovering the back-up seed or any information relating to the mnemonic phrase used in the seed creation.

(2) The revocation of a signatory shall only cause the removal of the signatory's access to a back-up seed without the need to create a new wallet or migrate the digital asset in custody to another wallet.

(3) A custodian shall monitor user access logs to ascertain any unauthorized access by revoked signatories.

(4) A custodian shall have the procedures mentioned in paragraph (1) audited on a yearly basis by an external independent third party.

29. Digital asset agnostic systems and procedures

The systems and procedures of a custodian shall be digital asset-agnostic and shall ensure the same level of regulatory compliance relating to the safekeeping, transaction management and custody operations of every digital asset type, irrespective of wallet functionality protocol.

30. Multi-Signature Authorisation

(1) The systems and procedures of a custodian shall ensure that no single person is able to initiate and complete a transaction pertaining to a digital asset being held in custody.

(2) A custodian shall be required to mitigate the risk of collusion between signatories in view of initiating unauthorized transactions relating to a digital asset under custody.

31. Selection of signatories

A custodian shall be required to have procedures in place in view of designating the signatories for transactions relating to digital asset under custody.

32. Justification for approval or rejection of a transaction

(1) A custodian shall ensure that the rationale for approving or rejecting a transaction in relation to a digital asset under custody is documented by each signatory.

(2) A custodian shall maintain proper records of the rationale for approving or rejecting any transaction.

(3) The records referred to in paragraph (2) shall be made available to the Commission and to the client upon request.

33. Detection of suspicious or fraudulent transactions

(1) A custodian shall have documented systems and procedures for detecting and reviewing suspicious or fraudulent transactions.

(2) The documented systems and procedures shall include remedial actions to be implemented following the findings of the review.

34. Financial statements

(1) A custodian shall file with the Commission quarterly financial statements relating to the custodial activities as soon as possible, but not later than 45 days after the closing date of the relevant quarter.

(2) A custodian shall, as soon as possible but not later than 90 days of its balance sheet date, file with the Commission audited financial statements prepared in accordance with IFRS and audited in accordance with the International Standards on Auditing and such other standards as may be issued under the Financial Reporting Act 2004.

35. Transactional Records

(1) A custodian shall ensure that, at all times, it has up to date transactional records including-

(a) transaction timestamp;

(b) transaction type;

(c) due diligence on parties to the transaction;

(d) relevant signatories and transaction approval/rejection evidence;

(e) account balances; and

(f) transaction value.

(2) The records referred to in paragraph (1) shall be made available for inspection by the Commission upon request.

36. Commencement

These rules shall be deemed to come into operation on 01 March 2019.

Made by the Financial Services Commission on 28 February 2019.

BY AUTHORITY: GOVERNMENT PRINTING DEPARTMENT, LA TOUR KOENIG 20/03/19 – 1150