

Rulebooks

Compulsory Rulebooks

Company Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Company Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out any VA Activity in the Emirate.

This Company Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out any VA Activity must also comply with the following Rulebooks applicable to all VASPs—

- Compliance and Risk Management Rulebook;
- Technology and Information Rulebook;
- Market Conduct Rulebook; and
- All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

Capitalised terms in this Company Rulebook have the meanings ascribed to them in the Regulations or as otherwise defined herein or provided in Schedule 1.

Unless otherwise stated, all requirements in this Company Rulebook are Rules and have binding effect.

Part I – Company Structure

Introduction

Parts I-III of this Company Rulebook govern the way a VASP structures and manages its company, Board, Senior Management and Staff and the ongoing maintenance of satisfactory internal control and management systems. Rules in Parts I-III of this Company Rulebook set out requirements regarding—

- company structure and Board structure;
- responsibilities of the Board and Senior Management;
- induction and training for the Board and Staff; and
- when individuals will be deemed to be Fit and Proper Persons.

The corporate governance needs of a VASP may vary from one to another depending upon a thorough analysis of its particular structure and business operations. The Board and the Senior

Management are ultimately responsible for the adequacy and effectiveness of the internal control system implemented for that VASP.

A. Company Ownership Structure

1. General requirement. VASPs shall maintain a company structure which is clear and transparent for the purposes of effective oversight by VARA and that ensures a sound and effective operation of the business of the VASP, including its VA Activities, which is conducive to the fair and orderly functioning of any market involving Virtual Assets.
2. Legal entity in the Emirate. VASPs shall have and maintain a legal entity in the Emirate in one of the legal forms approved by a commercial licensing authority in the Emirate.
3. Ownership. VASPs shall maintain a company structure with a clear chain of ownership, delegated authority and all associated voting powers, such that VARA can clearly identify any Controlling Entity(ies) and the Ultimate Beneficial Owners (“**UBOs**”).
4. Governance. If a VASP adopts a complex company structure including but not limited to trusts and nominee arrangements, and/or structures involving Decentralised Autonomous Organisations (“**DAOs**”) or other organisational forms with decentralised governance, then it is required to furnish information to VARA relating to the following, during the licensing process and at any time on request from VARA, for the purpose of VARA assessing the VASP’s compliance with Rule I.A.1 of this Company Rulebook—
 - a. the reason(s) for the adoption of such complex company structure and/or decentralised governance;
 - b. the relationship between the VASP and relevant DAOs and/or Entities with decentralised governance;
 - c. whether the inclusion of DAOs and/or Entities with decentralised governance in the Group or the VASP’s affiliation with such Entities may adversely impact the VASP’s ability to ensure compliance with Regulations, Rules and Directives (including what procedures are in place to ensure effective compliance decisions can be made by way of decentralised governance or voting mechanisms); and
 - d. whether the relevant DAOs and/or Entities with decentralised governance are registered or otherwise legally recognised as, or have within its structure, an Entity in any jurisdictions other than the Emirate.
5. VASPs shall obtain VARA’s written approval prior to any material change to their company structure (including Controlling Entity(ies) and UBOs) and/or adopting decentralised governance in respect of any of their operations relating to VA Activities. In respect of any such changes to its shareholding structure and/or governance model, a VASP shall—
 - a. provide the types of information as set out in Rule I.A.4 of this Company Rulebook (if applicable);
 - b. provide any additional due diligence information about new Controlling Entity(ies), Group Entities and UBOs as may be requested by VARA; and
 - c. comply with any additional conditions or restrictions that VARA may impose to ensure its ability to comply with all applicable laws and regulatory requirements is not impaired, including but not limited to the filing of declarations that any new Controlling Entity(ies) and UBOs are not Politically Exposed Persons or individuals who are subject to any form of economic sanctions.

B. The Board

1. Board structure.

- a. VASPs shall ensure the Board comprises suitably qualified individuals with the requisite skills, knowledge and expertise taking into consideration the scope of their responsibilities and the VA Activities carried out by the VASP. Each member of the Board must be assessed by the VASP and approved by VARA as being a Fit and Proper Person according to the criteria set out in Part III of this Company Rulebook.
- b. VASPs shall—
 - i. adopt a clear and effective procedure for—
 1. selecting and appointing members to the Board, including the filling of any vacancies on the Board;
 2. removal of members of the Board; and
 - ii. ensure that all procedures relevant to this Rule I.B.1.b of the Company Rulebook are included in the VASP's constitutional documents.
- c. The Board shall assess and confirm each member of the Board is a Fit and Proper Person at least annually. If a VASP has reason to believe a member of the Board no longer remains a Fit and Proper Person at any time, the Board shall promptly assess such member. If such member of the Board no longer remains a Fit and Proper Person, the Board shall remove such member with written notice and appoint a successor in accordance with Rule I.B.1.b of this Company Rulebook.
- d. VASPs shall ensure that any changes to the constitution of the Board comply with Rules I.B.1.a and I.B.1.b of this Company Rulebook.
- e. The Board shall establish a process to elect a chairman. The chairman shall have the authority to oversee and be responsible for the overall effective functioning of the Board, and any committees it has established, in accordance with Rule I.B of this Company Rulebook.
- f. The Board shall carry out annual assessments, alone or with the assistance of external experts, of the Board as a whole, its committees and individual members to review relevant performances.

2. Responsibilities of the Board.

- a. The Board shall establish and regularly update the VASP's procedural rules and other constitutional documents setting out its organisation, responsibilities and procedures.
- b. The Board and each of its members shall assume full responsibility for—
 - i. the operation, business and affairs of the VASP, such that these are conducted in a manner which is conducive to the fair and orderly functioning of any market involving Virtual Assets;
 - ii. the VASP's compliance with all applicable laws and regulatory requirements (including but not limited to Regulations, Rules and Directives); and
 - iii. implementing a professional compliance culture within the VASP.

- c. The Board shall engage in regular and effective communication with relevant committees, Senior Management, Staff, any other individuals within the VASP and Group Entities to ensure that it is continually and timely apprised of the status of the business, operations and financial position of the VASP.
- d. The Board shall establish and maintain detailed and clear policies and procedures—
 - i. to set out the process of authorisations within the Senior Management and its subordinates;
 - ii. to identify the authority of each member of the Senior Management; and
 - iii. to identify reporting lines of the Senior Management and its subordinates.
- e. In performing its duties in official capacity, the Board may delegate its authority to relevant committees and Senior Management. In doing so, the Board shall supervise its delegated authority and remain primarily responsible for its duties. The Board shall establish and maintain effective systems and procedures to supervise the Staff who act under the authority delegated by the Board.
- f. The Board shall, at least annually, review the performance of the VASP, the practical and professional experience and suitability of its members and the Senior Management in the context of the latest industry standards in the global Virtual Asset sector.
- g. The Board shall ensure that all Entities performing functions on behalf of the VASP and contractors hired by the VASP have access to, and understand adequate up-to-date information regarding, the applicable policies and procedures implemented within the VASP in acting in their official capacities.
- h. The Board shall—
 - i. define clear reporting requirements to ensure that internal and external reports can be prepared in a timely manner; and
 - ii. establish and maintain effective record retention policies to comply with all applicable laws and regulations and to enable the VASP, its auditors and other interested Entities such as VARA to carry out routine and ad hoc reviews or investigations.

3. Board training.

- a. VASPs shall ensure new Board members receive training programme(s) on their company structure, corporate governance, business and other subjects that would assist them in performing their duties, with a particular focus on—
 - i. the background, strategy and objectives of the VASP;
 - ii. the financial and operational aspects of the VASP's business, including its VA Activities;
 - iii. the obligations, duties, liabilities and rights of the members of the Board;
 - iv. the functions and obligations of any Board committees; and
 - v. key risks relating to the global Virtual Asset sector.
- b. The Board shall—
 - i. review the scope of the training programme and the accuracy of its contents annually; and
 - ii. revise the training programme if necessary.

- c. VASPs shall provide regular, timely and up-to-date training courses to all members of the Board in matters directly related to the interests of the VASP and Virtual Asset markets as a whole, including but not limited to matters set out in Rule I.B.3.a of this Company Rulebook.

C. Responsible Individuals

1. VASPs shall appoint two (2) individuals of sufficient seniority who shall be responsible for the VASP's compliance with all legal and regulatory obligations ("Responsible Individuals").
2. Each Responsible Individual shall be—
 - a. a full-time employee of the VASP;
 - b. a Fit and Proper Person;
 - c. a resident of the UAE or a holder of a UAE passport; and
 - d. notified to, and approved by, VARA during the licensing process.
3. VASPs shall ensure that its Responsible Individuals continue to meet the requirements in Rule I.C.2 of this Company Rulebook at all times, and shall validate and maintain a record of such validation on an annual basis.
4. VASPs must notify and seek approval from VARA prior to any change in their Responsible Individuals, except in the event of reasonably unforeseen circumstances, in such instances the VASPs must notify VARA immediately and provide information on how they will continue to meet the requirements with regard to Responsible Individuals.

D. Senior Management

1. VASPs shall establish, document and maintain a management structure which clearly sets out the roles, responsibilities, authority and accountability of the Senior Management.
2. VASPs shall ensure its Senior Management comprises suitably qualified individuals with the requisite skills, knowledge and expertise as may be reasonably expected in the global Virtual Asset sector.
3. The Board shall—
 - a. adopt a clear process and procedure for selecting and appointing members to the Senior Management; and
 - b. ensure that such process and procedure are included in the VASP's constitutional documents.
4. The Senior Management shall—
 - a. act under the direction and oversight of the Board; and
 - b. carry out and manage day-to-day activities of the VASP in a manner which—
 - i. complies with all applicable laws and regulatory requirements; and
 - ii. aligns with the business objectives and policies approved by the Board.
5. A member of the Senior Management may—

- a. except in the case of the Compliance Officer (“**CO**”) and/or the head of any internal audit functions, hold a position on the Board;
- b. subject to prior written approval of the Board and screening of conflicts of interest conducted by the Board, hold a position on the board of Entities other than the VASP; and
- c. not hold an employee position in any other Entities except with the prior written consent of the Board.

6. If a member of the Senior Management has been serving on the board of another Entity prior to joining the VASP, such member may continue to serve on the board of that Entity provided that the Board is satisfied that, after conducting relevant screening, no conflicts of interest would arise from the VASP’s appointment of such member.

7. The Senior Management shall furnish all necessary information that the Board may require to supervise and assess the performance of the Senior Management, which assessment shall be carried out by the Board at least annually.

E. Company Secretary

- 1. Notwithstanding any applicable requirements in the constitutional documents of the VASP, the Board must appoint a company secretary independent of the Senior Management, who reports directly to the Board (“**Company Secretary**”). The authorities and remuneration of the Company Secretary shall be determined under a Board resolution, unless the constitutional documents of the VASP provide otherwise.
- 2. The Company Secretary shall—
 - a. document the Board meetings and prepare their minutes, which shall include the discussions and deliberations that took place during these meetings, the place and start and end time of these meetings, registering the Board resolutions and voting results, and keeping them in a special and organised record, including the names of attendees and any expressed reservations. These minutes shall be signed by all attending members;
 - b. keep all reports submitted to the Board and those prepared thereby;
 - c. provide Board members with the Board meeting agenda of the meeting and the related papers, documents, and information and any additional information related to subjects contained in clauses of the agenda requested by any Board member;
 - d. make sure that Board members comply with actions approved by the Board;
 - e. notify Board members of the Board meetings dates well in advance of the meeting date;
 - f. submit drafts of the minutes to Board members to express their opinion thereon before signing it;
 - g. make sure that the Board members, completely and immediately, receive a full copy of the minutes of the Board meetings, information and documents related to each meeting;
 - h. keep the minutes of meetings of the Board and its committees;
 - i. inform Staff, including Senior Management, about resolutions of the Board and its committees relevant to their function or roles and report on their implementation and application;
 - j. support the Board in any activities or processes requested by the Board;
 - k. coordinate between Board members and Senior Management; and
 - l. regulate the disclosure record of the Board in accordance with applicable requirements in the Market Conduct Rulebook and provide assistance and advice to the Board members.

3. The Board may appoint an external Entity as Company Secretary provided that such appointment will be considered as an Outsourcing and must comply with Part IV of this Company Rulebook.

Part II – Corporate Governance

A. Competence

1. VASPs shall establish and maintain policies and procedures to ensure that all members of the Board, Senior Management and Staff are suitably qualified in their relevant post. Criteria for such internal assessment shall include, but are not limited to—
 - a. academic credentials;
 - b. professional qualifications;
 - c. professional experience;
 - d. awards and honours received; and
 - e. memberships of professional and service organisations.
2. The Board can only appoint to supervisory positions Staff with relevant experience and qualifications as may be reasonably expected taking into account the responsibilities of the role and the VA Activities of the VASP.

B. Segregation of Duties

1. The Board shall ensure that policy formulation, supervisory and advisory functions and other internal review functions are effectively segregated from operational duties in order to—
 - a. ensure that supervisory and other internal controls are effectively maintained; and
 - b. avoid undetected errors or abuses of certain functions.
2. The Board shall ensure that operational duties including sales, dealing, accounting, settlement and safekeeping of Virtual Assets are effectively segregated to minimise potential for conflicts, errors or abuses.
3. The Board shall ensure that compliance and internal audit functions are effectively segregated from and independent of the operational and related supervisory functions. The CO and any head of the internal audit function should report directly to the Board.

C. Conflicts of Interest

1. VASPs shall use all reasonable efforts to avoid conflicts of interest between any of the following—
 - a. their Group;
 - b. the VASP;
 - c. their Board;
 - d. their Staff;
 - e. their clients; and/or

f. their investors.

In the event that the VASP cannot avoid conflicts of interest after using all reasonable efforts, it shall ensure that such conflicts of interest are disclosed to its affected clients, and such clients should be fairly treated by the VASP.

2. If a VASP, a member of the Board or any of its Staff has an interest that may reasonably impair its objectivity, in a transaction with or for a client or a relationship which gives rise to an actual or potential conflicts of interest in relation to the transaction, the VASP shall—
 - a. promptly disclose the nature of such conflict to its affected client; and
 - b. to the extent that the affected client's interests can be sufficiently protected, manage and minimise such conflict by adopting appropriate measures to ensure fair treatment to its affected client, including establishing and maintaining information barriers to separate Staff into different teams.
3. VASPs shall establish and implement appropriate written internal policies and procedures for the identification and management or resolution (as applicable) of any actual or potential conflicts of interest. VASPs shall maintain a special register for conflicts of interest in which the conflicts and management or remedial measures taken are recorded in detail.
4. When a member of the Board discloses to the Board that they have a material interest in a transaction, the remaining members of the Board present at the Board meeting shall consider whether it is appropriate for that Board member to continue to participate in the Board meeting after reviewing whether the conflict may affect the objectivity of that member and/or their ability to perform their tasks towards the company properly. If the remaining members of the Board decide that it is not appropriate for that member to participate, they may ask that member to leave the Board meeting. That Board member is not entitled to use the member's personal influence in issues whether in or outside the meeting. The Board member shall not vote on the decision. The Company Secretary shall record the conflict in the relevant Board minutes.
5. Where a VASP represents itself as being independent when conducting a VA Activity—
 - a. it shall not receive fees, commissions or any benefits, paid or provided (whether directly or indirectly) by any Entity other than the end client in relation to the provision of services related to such VA Activity to clients; and
 - b. it shall not have any close links or other legal or economic relationships with third parties which are likely to impair its independence to favour a particular third party in relation to its provision of services related to such VA Activity.

D. Information Disclosure

1. The Board shall establish and maintain effective policies and procedures to disclose all necessary information to the VASP's shareholders and relevant stakeholders clearly, correctly and in an orderly manner in order to obtain a comprehensive view of the overall performance and financial position of the VASP.
2. The website of the VASP shall include all information required to be disclosed to the public in accordance with all applicable laws, Regulations, Rules and Directives, including but not limited to all public disclosures required under the Market Conduct Rulebook and all other Rulebooks applicable to the VASP, and any other details and information that can be published through other disclosure methods.
3. The Board shall review the VASP's disclosure policies and procedures periodically, and ensure and procure its compliance to the best practices in the Virtual Asset industry.

E. Group Governance

1. VASPs shall establish a framework for governing their Subsidiaries within the Group. The Board shall be responsible for determining how Subsidiary governance is addressed and conducted.
2. The Board shall approve the governance framework for the Subsidiaries that sets out the powers within the Subsidiaries and ensure that the boards of the Subsidiaries implement the governance framework for their respective Subsidiary.
3. The governance framework shall include—
 - a. planning of the rights and the roles of the VASP;
 - b. company policies and procedures adopted by the Subsidiaries;
 - c. participation of the Board with the boards of the Subsidiaries prior to the VASP exercising its right to elect members to the boards of the Subsidiaries; and
 - d. restrictions imposed on the Board members not to use any information obtained as a member of the board of a Group Entity for the purposes of another company within the Group.
4. VASPs shall verify the performance of the governance framework of the Subsidiaries.

F. Insiders' Transactions

1. The Board shall implement rules to govern and monitor the transactions of Board members and its Staff in order to ensure compliance with the Regulations and the Market Conduct Rulebook.

G. Transactions with Related Parties

1. VASPs shall not enter into transactions with any Related Party without the prior written consent of the Board where the value of the transaction exceeds five percent (5%) of their issued share capital. If there is a significant change to the terms of these transactions, further written consent of the Board is required before the VASP enters into the transaction under the changed terms.
2. The Related Party who has an interest in a transaction described in Rule II.G.1 of this Company Rulebook shall not participate in voting in terms of the decision taken by the Board in respect of such transactions.
3. The following Entities shall be liable for damages to the VASP if a transaction with a Related Party is concluded in contravention of this Rule II.G of the Company Rulebook, or if it is proven that the transaction is unfair or involves a conflict of interest and incurs damages or otherwise detrimental to the best interests of the VASP's shareholders—
 - a. that Related Party with whom the transaction was entered into; and
 - b. the Board if the decision was issued by consensus.
4. If the decision was only issued by the majority of the Board, the dissenting Board members shall not be held liable in the event that they have recorded their objection in the Board minutes. If a Board member is absent from the meeting in which the decision was issued, they are still responsible for the decision unless they prove that they were unaware of the decision or if they had constructive knowledge of it but could not object thereto.

5. In the event that a VASP enters into a transaction with a Related Party—
 - a. the Board shall provide VARA with prior notice which shall identify the Related Party and provide details of the transaction, including the nature and the benefit of the involvement of that Related Party in the transaction, together with a written confirmation that the terms of the transaction with that Related Party are fair, reasonable, and proportional to the interests of the shareholders of the VASP;
 - b. it shall allow clients and shareholders to review its company records and any documents relating to those transactions; and
 - c. VARA and/or the VASP's clients and shareholders may take or join any legal action before a competent court regarding the transactions concluded with that Related Party to compel the parties of the transaction to provide all information and documents relating to those transactions, whether directly to prove the facts set out in the case relevant to it or to lead to the discovery of information that will help in the detection of the facts, and seek cancellation of the transaction and oblige that Related Party to return the profit or benefit gained back to the VASP, in addition to any compensation ordered to be payable by that Related Party.
6. VASPs shall maintain a register of transactions with Related Parties where the names of such Related Parties shall be recorded together with relevant transactions and actions taken in relation thereto in detail.
7. In addition to the requirement in Rule II.G.6 above and all other reporting requirements in the Compliance and Risk Management Rulebook, VASPs shall report all transactions with Related Parties to VARA monthly, or otherwise upon request by VARA, including the details of those transactions.
8. VASPs shall provide any documents and other information relating to transactions with Related Parties as reasonably requested by VARA to for the purposes of supervising the VASP's compliance with this Rule II.G of the Company Rulebook.

H. Loans to the Board or Staff

1. VASPs shall notify VARA and obtain approval prior to making any loan to a member of the Board, Senior Management or Responsible Individual.
2. When making such notification, VASPs shall include full details of—
 - a. the name of the member of the Board, Senior Management or Responsible Individual receiving the loan;
 - b. the amount of the loan; and
 - c. the purpose of the loan.

Part III – Fit and Proper Requirements

A. General Principles

1. A Fit and Proper Person must—
 - a. possess the necessary academic qualifications and in all cases, have relevant professional knowledge and/or industry qualifications, in each case, having regard to the nature of the functions to be performed;

- b. be honest, reputable, have integrity and uphold the ethical standards reasonably expected of their role;
- c. possess adequate relevant global Virtual Asset sector and management experience, or such experience in another relevant sector;
- d. possess a good understanding of the regulatory framework which governs the nature of the job or role and the market; and
- e. be financially sound.

2. In assessing whether an individual is a Fit and Proper Person, VASPs should consider—

- a. the nature, scale and complexity of their business, including all VA Activities, and the nature and range of activities undertaken by such individual in the ordinary course of business; and
- b. whether such individual has the knowledge, skills, and experience to perform the specific role that the individual is intended to perform.

3. In assessing an individual for a position within the Board, VASPs should ensure that, if such individual is appointed to the Board, the Board as a whole will at all times possess adequate knowledge, skills and experience to undertake the business activities of the VASP.

4. In assessing whether an individual is a Fit and Proper Person, VARA will—

- a. consider all relevant factors in assessing the application of the fit and proper principles contained herein on a case-by-case basis, taking into account—
 - i. the conditions of the Licence held by the VASP;
 - ii. the business model of the VASP;
 - iii. the market within which the VASP operates;
 - iv. the governance structure, the internal control systems and the competence of the VASP's Staff;
 - v. decisions made by a relevant authority or regulatory body in respect of that individual, whether in the Emirate or in other jurisdictions;
 - vi. the state of affairs of any other business which that the individual carries on or proposes to carry on; and
- b. look to the substance of the requirements and the materiality of any failure to meet such requirements.

5. VARA will not grant approval if it is not satisfied that the individual is a Fit and Proper Person.

6. If an individual does not meet any individual elements set out in Part III of this Company Rulebook, VARA may nonetheless be satisfied that such individual is a Fit and Proper Person taking into account all relevant factors.

B. Qualification

1. In assessing whether an individual is a Fit and Proper Person and qualified for the role for which the individual is being considered, the following factors shall be considered—

- a. whether the individual possesses a degree in the field relevant to the role. For the avoidance of doubt, this does not prevent someone who does not possess a degree in the

relevant field to be employed for the role if such individual has relevant professional or industry qualification(s) and/or experience; and

b. whether the individual has industry qualifications directly relevant to the activities to be performed by such individual in the role and it is demonstrable that such individual generally understands—

- i. the structure of the regulatory framework that applies to the job activities;
- ii. the particular Regulations, Rules, Directives and Guidance that apply to the functions that the individual would perform;
- iii. the fiduciary obligations owed to clients by the individual or the VASP;
- iv. the VA Activities which the individual helps the VASP to undertake; and
- v. the market in which the individual's services are provided.

C. Industry Experience

1. Relevant industry experience refers to hands-on working experience acquired through the carrying on of VA Activities in the Emirate or activities of a similar nature in other industries and/or jurisdictions.
2. In assessing the relevance of an individual's experience, VASPs must consider whether the substance of the experience is directly relevant or crucial to the VA Activities to be carried out by such individual.
3. In assessing whether an individual has sufficient relevant industry experience, VASPs may consider such individual's overall career history accumulated as a whole.

D. Management Experience

1. In assessing whether an individual has management experience suitable for a role in the Board or the Senior Management, VASPs must consider whether such individual has hands-on working experience in supervising and managing essential VA Activities and staff in a business setting. To this end, management experience which is purely administrative would be less relevant.

E. Financial Status or Solvency

1. An individual will not be considered to be a Fit and Proper Person if such individual—
 - a. is an undischarged bankrupt, currently subject to bankruptcy proceedings or a bankrupt who has recently been discharged;
 - b. is subject to receivership or other similar proceedings; and
 - c. has failed to meet any judgment debt, having regard to the circumstances of such failure and the recency of such failure.

F. Honesty, Integrity and Reputation

1. In assessing an individual's honesty, integrity and reputation, VARA will have regard to all matters it deems relevant, including, but not limited to, the following, which may have occurred in the Emirate or in other jurisdictions—

- a. whether the individual has been convicted of any criminal offence, with particular consideration given to offences of dishonesty, fraud, financial crime or an offence under laws relating to companies, banking, insolvency, money laundering and insider dealing;
- b. whether the individual has been the subject of any adverse finding or any settlement in civil proceedings, with particular consideration given to investment or other financial business, misconduct, fraud or the formation or management of a body corporate;
- c. whether the individual has been the subject of any existing or previous investigation or disciplinary proceedings or has been notified of any potential disciplinary proceedings or any investigation which might lead to those proceedings;
- d. whether the individual is or has been in breach of any regulatory requirements;
- e. whether the individual has been the subject of any justified complaint relating to VA Activities or similar business activities in any jurisdiction;
- f. whether the individual has been a director or a member of the senior management of a business that has gone into insolvency, liquidation or administration while the individual has been connected with that business or within one (1) year of that connection;
- g. whether the individual has been a party to a scheme of arrangement or entered into any form of compromise with a creditor involving any amount greater than AED 50,000;
- h. whether the individual has been dismissed for cause from employment or from a position of trust, fiduciary appointment, or otherwise found to be deficient in discharging their duties;
- i. whether the individual has been disqualified from acting as a director or in any managerial capacity; and
- j. whether, in the past, the individual has been candid and truthful in all dealings with any regulatory body and whether the individual demonstrates a readiness and willingness to comply with the requirements and standards of the regulatory system and all other applicable laws and regulatory requirements.

2. For the avoidance of doubt, conviction for a criminal offence would not automatically bar an individual from being a Fit and Proper Person. VARA may consider the seriousness of the prior conviction and the circumstances surrounding the offence, including the explanation offered by such individual, the relevance of the offence to the individual's role, the passage of time since the offence was committed, evidence of such individual's rehabilitation, and any measures or controls the individual and/or the VASP will have in place in response to such conviction.

3. In considering the reputation of an individual, VARA shall consider whether the individual's reputation has or might have an adverse impact upon the performance or perception in the market of the VASP.

G. Continuing Requirements

1. When VASPs assess whether an individual remains a Fit and Proper Person, they shall assess the role such individual is actually performing at the time the assessment is done.
2. In addition to all of its other powers of enforcement, if VARA is of the view that an individual is no longer a Fit and Proper Person, it may—
 - a. revoke or suspend the approval granted to such individual or the Licence of the relevant VASP;
 - b. publicly or privately reprimand such individual;
 - c. prohibit such individual from applying again;
 - d. impose a fine or other non-financial penalties in the event of a material breach of this Part III of the Company Rulebook;

- e. require the VASP to implement additional measures or controls; and
- f. take any other enforcement action as determined by VARA.

Part IV – Outsourcing Management

Introduction

Whilst VARA recognises the potential benefit to VASPs of Outsourcing certain business activities to third-party Service Providers, Outsourcing poses a number of challenges from an operational and regulatory perspective. Outsourcing may increase a VASP's dependency on a third party and potentially reduce its control over proprietary and client-related information and systems. This creates risks for the VASP in respect of business disruption, security of data and, in some cases, may create risks to investors in Virtual Assets and the wider market.

A. Application & Scope

1. Application & scope
 - a. *In scope*

Subject to Rules IV.A.1.b and IV.A.1.c, this Part IV shall apply to all Outsourcing arrangements of VASPs.
 - b. *Out of scope*

The following shall not be treated as Outsourcing—

 - i. a Function that is legally required to be performed by a Service Provider (e.g. statutory audit);
 - ii. market information services (e.g. provision of data);
 - iii. global network infrastructures; and
 - iv. the acquisition of services that would otherwise not be undertaken by the VASP (e.g. advice from a lawyer, cleaning and gardening, post-room services, receptionists and switchboard operators), goods (e.g. office supplies, furniture) or utilities (e.g. electricity, gas, water, telephone line).
 - c. *Non-core systems or business*

An Outsourcing by a VASP to a Service Provider in relation to non-core systems which do not relate to its core business, or any service or task where a defect or failure in their performance would not materially impair the continuing compliance by the VASP with its Licence including all conditions, shall not fall within the scope of this Part IV of the Company Rulebook.
2. Prohibited Outsourcing. VASPs must not enter into any Outsourcing arrangement that would materially impair—
 - a. the quality of their internal controls; or

- b. the ability of VARA and other competent authorities to exercise their statutory rights or to monitor, supervise or audit the VASP's compliance with all applicable laws or regulatory requirements.
- 3. Specified officers. VASPs may enter into Outsourcing arrangements with respect to each of their MLRO, CISO and/or Data Protection Officer, provided that—
 - a. any such Outsourcing complies with this Part IV of the Company Rulebook at all times;
 - b. individuals appointed to any of the roles of MLRO, CISO and/or Data Protection Officer agree to individual responsibility to VARA during the licensing process or prior to being appointed;
 - c. to the extent that such individual holds roles with more than one (1) VASP, VARA shall take this into consideration when assessing the individual's ability to perform the duties required of their role and may impose requirements on the individual to maintain separation between such roles, including but not limited to implementing information barriers; and
 - d. whilst VASPs can Outsource such roles, they are encouraged to resource them in-house and VARA may in its sole discretion require a VASP to resource any of those roles with a full-time employee, either during the licensing process or any time thereafter.
- 4. Outsourcing - other legal and regulatory obligations.
 - a. To the extent applicable, VASPs must comply with the CBUAE *Circular No. (14) of 2021 Outsourcing Regulation for Banks*, as may be amended from time to time.
 - b. VASPs must also consider, to the extent applicable to its Outsourcing arrangements—
 - i. guiding principles for Outsourcing in financial services issued by the Technical Committee of the International Organisation of Securities Commissions, the Basel Committee on Banking Supervision, or any other international body promulgating standards for Outsourcing by financial services providers; and
 - ii. any equivalent principles or regulations applicable to the VASP's Group in other jurisdictions.
 - c. Notwithstanding the above, VASPs must comply with all Rules, Directives and Guidance with respect to Outsourcing as may be specified by VARA from time to time, which shall supersede the other guidance and regulations mentioned in this Rule IV.A.4 of the Company Rulebook.
- 5. Accountability. VASPs shall be ultimately responsible for compliance with their legal and regulatory obligations and shall be accountable to VARA for any and all Functions that such VASPs may Outsource to a Service Provider to the same extent as if the Function was performed in-house by the VASP.

B. Risk Assessment, Due Diligence and Controls

- 1. Risk based approach. VARA recognises that Outsourcing arrangements exhibit a varying degree of risk and expects VASPs to take this into account in assessing and managing the relevant risks. Measures taken by a VASP must be commensurate with the degree of risk associated with the Outsourcing arrangements. Material Outsourcings shall be subject to additional requirements as set out in this Part IV of the Company Rulebook.

2. Risk assessments.

- a. VASPs should have a process to assess the risk in relation to each Outsourcing arrangement they propose to enter into (including the variation or renewal of Outsourcing arrangements) and to identify if any such Outsourcing constitutes a Material Outsourcing. This assessment should be conducted prior to the commencement of an Outsourcing relationship and at least annually for the duration of such relationship.
- b. In respect of Outsourcing arrangements, the assessment of risk is dependent on the specific circumstances of each VASP. In assessing risk, factors that should be considered include, but are not limited to, the following—
 - i. impact on the financial position, business operation, continuity of services, clients' best interests, and reputation of the VASP upon the Service Provider's failure to perform;
 - ii. impact of the Outsourced activity on the ability of the VASP to comply with legal and regulatory requirements;
 - iii. the scope, complexity and criticality of the service to be Outsourced;
 - iv. impact of the Outsourced activity on internal control Functions of the VASP;
 - v. cost of Outsourcing as a proportion to the total operating costs of the VASP;
 - vi. the regulatory status of the Service Provider;
 - vii. risks that are relevant to the geographical location of a Service Provider, including but not limited to those contained in Rule IV.F of this Company Rulebook; and
 - viii. the degree of difficulty and time required to find an alternative Service Provider or to bring the Outsourced service in-house.

3. Due diligence.

- a. Prior to selecting a Service Provider, VASPs must perform detailed due diligence in relation to the Service Provider to ensure that the Service Provider has the ability and capacity to undertake the provision of the Outsourcing effectively, reliably and to a high standard. This should include an assessment of the Service Provider's quality of services, technical, managerial and human resources capacity, financial soundness, reputation and experience, licensing or regulatory status, extent of reliance on and control of subcontractors, compatibility with the VASP's corporate culture and business strategies, familiarity with the Virtual Asset industry and capacity to keep pace with innovation in the market. Other considerations that may be relevant include aggregate exposure to a particular Service Provider, costs and possible conflicts of interest.
- b. During the conduct of an Outsourcing, VASPs should regularly (and in any event at least annually and as circumstances warrant) review the selected Service Provider to ascertain whether the Service Provider remains competent to provide the Outsourced service to the standards required.

C. Internal Governance – Outsourcing Policy and Register

1. Prior to the Outsourcing of services and on an ongoing basis, VASPs should establish and maintain comprehensive Outsourcing policies, contingency plans and Outsourcing risk management programmes (“**Outsourcing Policy**”).
2. Outsourcing Policy.

- a. An Outsourcing Policy should include, but not be limited to the following—
 - i. the framework for a comprehensive assessment of risks involved in Outsourcing and identifying whether a proposed Outsourcing is a Material Outsourcing or not;
 - ii. procedures for identifying, measuring, managing, mitigating, controlling and reporting the risks of an Outsourcing arrangement and any conflicts of interest;
 - iii. the objectives of the Outsourcing and criteria for approving an Outsourcing arrangement;
 - iv. procedures that clearly identify the Staff involved in the VASP and their roles and responsibilities with regard to Outsourcing arrangements;
 - v. procedures that clearly identify the responsibilities of each party in respect of the Outsourcing and in particular what responsibilities have been retained by the VASP;
 - vi. procedures to deal effectively with any act or omission by the Service Provider that leads, or might lead, to a breach of any law or regulation, and enact required remediation measures promptly; and
 - vii. a review mechanism to ensure the Outsourcing policy can be updated as necessary to align with industry and regulatory developments as well as the VASP's strategic development needs.
- b. VASPs must maintain a comprehensive register of all Outsourcing arrangements, including both those of the VASP itself and its Group, which must include the following key information for each Outsourcing arrangement, at a minimum—
 - i. the name of each Service Provider;
 - ii. a description of the scope of the Outsourced service;
 - iii. location where the Outsourced service is being performed;
 - iv. start and end date of the Outsourcing agreement;
 - v. key points of contact for the Service Provider;
 - vi. whether the Outsourcing arrangement is a Material Outsourcing;
 - vii. whether the Outsourcing involves storage or processing of Personal Data (beyond the exchange of business contact information between the VASP and the Service Provider for administration purposes); and
 - viii. whether the Outsourcing arrangement involves any confidential information.

3. Oversight of Outsourcing – monitoring the service.

- a. VASPs must manage identified risks associated with the Outsourcing activity and such Service Provider's compliance with its contractual obligations as well as managing their relationship with the Service Provider, having regard to the risks presented by the Outsourced activity to the ongoing business of the VASP and its regulatory obligations.
- b. Monitoring should be assigned to Staff with appropriate expertise and cover the Service Provider's contractual performance, financial soundness and risk profile, any material issues encountered in the provision of services and any remedial steps and mitigation measures taken in respect thereof. The monitoring and control processes and procedures of VASPs should be subject to regular reviews and audits to evaluate effectiveness and adequacy.

D. Outsourcing Agreements

1. VASPs must ensure all Outsourcing arrangement are undertaken in the form of a legally binding written agreement which clearly sets out the relevant rights, liabilities and obligations of the Service Provider and the VASP. The contents and level of contractual protection required should reflect the risk level of the Outsourcing arrangement. VASPs should regularly review their Outsourcing agreements to assess whether it is necessary to renegotiate provisions to bring the agreements in line with current market standards and changes in the VASP's business development strategies.
2. The following matters should be taken into consideration by the VASP when negotiating the provisions of any Outsourcing agreement—
 - a. performance standards to be achieved in respect of the Outsourced service, and consequences for failing to achieve such standards;
 - b. delineation of intellectual property, proprietary information and asset ownership and rights;
 - c. business continuity and contingency planning for the Outsourced service;
 - d. controls and process for changes to the Outsourcing arrangement;
 - e. guarantees or indemnities from the Service Provider; and
 - f. mechanism to resolve disputes that might arise under the Outsourcing arrangement.
3. Mandatory provisions for any Outsourcing. The following matters must be included in all legal agreements governing an Outsourcing—
 - a. a clear description of the Outsourced Function to be provided;
 - b. contractual assurance that the Service Provider is able to maintain processes and procedures for the continuous operation of the Outsourcing required by the VASP, in line with all applicable laws and regulatory requirements;
 - c. contractual requirements to maintain an appropriate level of information security, risk management and service delivery commensurate with the profile of the Outsourcing arrangement;
 - d. contractual requirements to protect confidential information and client data (as further specified in Rule IV.D.5 of this Company Rulebook below);
 - e. provisions allowing that the data that is owned or controlled by the VASP can be accessed at any time by the VASP or a competent authority and, in particular, in the case of resolution or discontinuation of business operations of the Service Provider or if it is insolvent;
 - f. notwithstanding Rule IV.E of this Company Rulebook below, conditions to be imposed in relation to sub-Outsourcing;
 - g. clearly set out the obligations of existing Service Provider on termination to securely destroy data relating to the VASP or its clients; and
 - h. the Outsourcing agreement should expressly allow the VASP to terminate the arrangement, in accordance with applicable laws, including in the following situations—
 - i. where the Service Provider is in breach of applicable laws, regulations or in material breach of contractual provisions;
 - ii. where there are material weaknesses regarding the management and security of confidential, personal or otherwise sensitive data or information; and
 - iii. where instructions are given by a competent authority (including VARA) to terminate the Outsourcing agreement or where such competent authority expresses significant concern regarding the adequacy or prudence of any such Outsourcing agreement.
4. Mandatory provisions for a Material Outsourcing. In addition to the mandatory provisions set out in Rule IV.D.3 of this Company Rulebook above, the following matters must be included in any

legal agreement governing a Material Outsourcing—

- a. the start date and end date, where applicable, of the agreement and the notice periods for the Service Provider and the VASP;
- b. the parties' financial obligations;
- c. the right of the VASP to monitor the Service Provider's performance on an ongoing basis;
- d. the agreed service levels or performance standards, which should include precise performance targets for the Outsourced Function to allow for timely monitoring so that appropriate corrective action can be taken without undue delay if the agreed service levels are not met, including consequences if service levels or performance standards are not met;
- e. the reporting obligations of the Service Provider to the VASP, including—
 - i. the communication (without undue delay) by the Service Provider of any breach of the VASP's data (including confidential information); or
 - ii. any development that may have a material impact on the Service Provider's ability to effectively carry out the Material Outsourcing in line with the agreed service levels, in compliance with all applicable laws and regulatory requirements and, as appropriate, the obligations to submit reports of the internal audit Function of the Service Provider;
- f. the requirements to implement and test business contingency plans;
- g. the obligation of the Service Provider to cooperate with the competent authorities of the VASP, including other Entities appointed by them;
- h. the right of the VASP and competent authorities to inspect and audit the Service Provider as further specified in Rule IV.G.2 of this Company Rulebook;
- i. termination and exit assistance arrangements to ensure the smooth transfer of the Outsourced service either to another Service Provider or back to the VASP with minimal disruption. To this effect, the Outsourcing agreement should—
 - i. clearly set out the obligations of the existing Service Provider in providing cooperation, reasonable assistance and transitional services on termination of the Outsourcing agreement, including the return, destruction or transfer of data; and
 - ii. include a transition period, where necessary, during which the Service Provider, after the termination of the Outsourcing arrangement, continues to provide the service to reduce disruption;
- j. the requirement for the Service Provider to hold relevant and adequate insurance; and
- k. the location(s) (i.e. regions or countries) where Material Outsourcing will be provided and/or where relevant data will be kept and processed, including the possible storage location, and the conditions to be met, including a requirement to notify the VASP if the Service Provider proposes to change the location(s).

5. Client confidentiality and data.

- a. VASPs must take appropriate steps to monitor their relationships with Service Providers and ensure that adequate measures are taken to safeguard the confidentiality and integrity of client data.
- b. Notwithstanding all other requirements in the Technology and Information Rulebook, VASPs must ensure that Outsourcing arrangements comply with all applicable UAE laws and regulations in respect of managing and processing data (e.g. the PDPL). This includes

requiring the Service Provider to procure, in the event a Service Provider subcontracts part of the service to a sub-contractor, the sub-contractor's compliance with all applicable laws and regulations. VASPs should ensure Service Providers are not permitted to provide any third party with access to confidential data of the VASP or its clients without obtaining the VASP's prior written consent.

- c. VASPs should take into account any applicable legal, regulatory or contractual obligations to notify clients or any competent authority in the event of an unauthorised data access or breach. In the event of an unauthorised data access or breach, where the VASP is required to notify clients or a competent authority under applicable legal or regulatory obligations, the VASP shall notify VARA within the same legally required time periods.
- d. VASPs should ensure that all client data should be destroyed or returned to the VASP in event of any termination of the Outsourcing arrangements, subject to applicable laws and regulatory requirements (e.g. recordkeeping requirements).

E. Sub-Outsourcing

- 1. Before entering into any Outsourcing arrangements, VASPs must consider the additional risk that may be posed if the Service Provider is allowed to further contract part of the service to third parties.
- 2. Sub-Outsourcing – all Outsourcing arrangements.
 - a. Consent should be given to sub-Outsourcing only if the subcontractor undertakes to—
 - i. comply with all applicable laws, regulatory requirements and contractual obligations; and
 - ii. provide the same contractual rights of access and audit as those granted to the VASP and where applicable its regulators (including VARA) by the Service Provider.
 - b. VASPs should ensure that no sub-Outsourcing engaged by the Service Provider will impede the Service Provider's ability to comply with its contractual obligations to the VASP, including requirements on confidentiality of client data, information access and audit rights, and business continuity planning.
- 3. Sub-Outsourcing – Material Outsourcing. The following requirements apply in relation to sub-Outsourcing in relation to all or part of a Material Outsourcing—
 - i. the Outsourcing agreement should specify whether or not sub-Outsourcing is permitted; and
 - ii. if sub-Outsourcing is permitted, the written Outsourcing agreement should—
 - 1. specify any types of activities that are not permitted to be sub-Outsourced;
 - 2. specify the conditions to be complied with in the case of sub-Outsourcing;
 - 3. specify that the Service Provider is obliged to oversee those services that it has subcontracted to ensure that all contractual obligations between the Service Provider and the VASP are continuously met;
 - 4. include an obligation of the Service Provider to inform the VASP of any planned sub-Outsourcing, or material changes thereof, in particular where that might affect the ability of the Service Provider to meet its responsibilities under the Outsourcing agreement;

5. ensure, where appropriate, that the VASP has the right to object to an intended sub-Outsourcing, or material changes thereof, or that explicit approval is required; and
6. include provisions such that the VASP has the contractual right to terminate the agreement in the case of undue sub-Outsourcing (e.g. where the sub-Outsourcing materially increases the risks for the VASP or where the Service Provider sub-Outsources without notifying the VASP).

F. Cross-Border Outsourcing

1. VASPs must take into account additional considerations in respect of Outsourcing to a Service Provider located outside of the UAE, including but not limited to the following factors in respect of the relevant jurisdiction which may affect the ability of an overseas Service Provider to fulfil the terms of an Outsourcing agreement or the ability of the VASP to monitor and control the Outsourced Function—
 - a. economic, political or social conditions;
 - b. differing legal or regulatory systems;
 - c. sophistication of the technology and infrastructure; and
 - d. reputational risk.
2. VASPs must take active steps in managing such risks, including conducting additional due diligence on potential Service Providers located outside of the UAE to understand whether they will be able to safeguard confidential information and client data and effectively monitor the overseas Service Provider, as well as execute business continuity plans and exit arrangements. VASPs must ensure, by means of adequate contractual and practical arrangements, that overseas Service Providers implement and maintain robust and appropriate levels of information security and service delivery throughout the duration of the Outsourcing relationship.
3. VASPs must ensure all applicable data protection laws are complied with in cross-border Outsourcing arrangements, including those in respect of international transfers of Personal Data.
4. VASPs should consider the need to notify (and obtain consent from) their clients in respect of cross-border Outsourcing arrangements, including the jurisdiction in which the service is to be performed and any rights of access available to overseas authorities.
5. In circumstances where an overseas authority requests access to the VASP's information, the VASP should notify VARA and any affected clients as soon as possible, subject to the VASP's compliance with applicable laws.
6. VASPs must notify VARA prior to undertaking any cross-border Outsourcing and must ensure that the Outsourcing arrangement would not impede VARA's ability to exercise its statutory rights and responsibilities, such as the rights of access and audit to information of the VASP.

G. Audit Rights

1. Audit rights – all Outsourcing arrangements. VASPs should ensure within the written Outsourcing arrangement that it is able to review the Outsourced Function. The written Outsourcing arrangements should refer to the information gathering and investigatory powers of competent authorities under applicable laws, and VASPs should also preserve those rights with regard to Service Providers located in third countries.
2. Audit rights – Material Outsourcing. VASPs should ensure within the written Outsourcing agreement in relation to a Material Outsourcing that they and their competent authorities (including VARA), and any other Entity appointed by them or the competent authorities, are

granted, the following—

- i. full access to all relevant business premises (e.g. head offices and operation centres), including the full range of relevant devices, systems, networks, information and data used for providing the service, including related financial information, personnel and the Service Provider's external auditors; and
- ii. unrestricted rights of inspection and auditing related to the Outsourcing arrangement, to enable them to monitor the Outsourcing arrangement and to ensure compliance with all applicable regulatory and contractual requirements.

3. Pooled audits.

- a. Without prejudice to their ultimate responsibility regarding Outsourcing arrangements, VASPs may use—
 - i. pooled audits organised jointly with other clients of the same Service Provider and performed by them and these clients or by a third party appointed by them, to use audit resources more efficiently; and
 - ii. third party certifications and third party or internal audit reports, made available by the Service Provider, if they ensure that the scope of the certification or audit report covers the systems, key controls and the compliance with relevant regulatory requirements and assess the content of the certifications or audit reports on an ongoing basis and verify that the reports or certifications are valid, adequate and current.
- b. VASPs should assess whether third-party certifications and reports as referred to in Rule IV.G.3 of this Company Rulebook are adequate and sufficient to comply with their regulatory obligations and should not rely solely on these reports over time. VASPs should also retain the contractual right to perform individual audits at their discretion with regard to the Material Outsourcing.

H. Regulatory Notifications

- 1. Notwithstanding all other notification requirements set out herein, VASPs must immediately notify VARA when they become aware of a material breach of the terms of a Material Outsourcing agreement they have with any Service Provider, or other material development in respect of a Material Outsourcing arrangement that has, or is likely to have, a significant impact on the operations, financial condition or reputation of the VASP.
- 2. VASPs are required to notify VARA immediately of any issues that may have arisen that would materially affect their compliance with their legal and regulatory obligations.
- 3. When a VASP intends to enter into any new Material Outsourcing arrangement or materially vary an existing Material Outsourcing arrangement, the VASP should notify VARA in advance providing relevant details of any such arrangement or amendment. In their notifications, VASPs should seek to satisfy VARA that all requirements of this Part IV of the Company Rulebook have been taken into account and properly addressed in its Material Outsourcing arrangements.
- 4. VARA may object to any Material Outsourcing and/or raise areas of concern, which the VASP must remedy to VARA's satisfaction prior to entering into any new Material Outsourcing arrangement or materially varying an existing Material Outsourcing arrangement.

Part V – Environmental, Social and Governance

Introduction

This Part V sets out:

- Environmental, social and governance (“**ESG**”) disclosure requirements; and
- Potential scope and direction of further regulation of ESG by VARA.

VARA acknowledges the importance of regulating and managing the ESG impact of VASPs, Virtual Assets and VA Activities. Accordingly, VARA will continue to monitor appropriate ways to regulate such impact and shall issue further Rules or Guidance where required.

A. Application

1. VASPs shall satisfy ESG disclosure requirements as set out in this Part V of the Company Rulebook.
2. During the licensing process, VARA will determine the ESG disclosure level required of each VASP, which shall be communicated to the VASP by VARA and required as a condition of the VASP’s Licence.
3. In making such determination, VARA may consider, but shall not be limited to, the following factors with respect to the VASP and its Group—
 - a. the number of Staff members or other personnel engaged by the VASP;
 - b. turnover and/or other financial information; and
 - c. business models and VA Activities.
4. VASPs may choose at any time to comply with a higher ESG disclosure level than that set by VARA as a condition of its Licence.
5. To the extent possible, VASPs should maintain the same ESG standard across its Group. Notwithstanding the preceding provisions of this Rule V.A of the Company Rulebook, such standards should be set and maintained at the highest level of any jurisdiction which is applicable to a VASP’s Group, including in respect of the VASP’s activities in the Emirate.

B. ESG Disclosure Levels

1. VARA has established three different levels of ESG disclosure requirements, which it may add to or amend from time to time—
 - a. Voluntary ESG Disclosure;
 - b. Compliance ESG Disclosure; and
 - c. Mandatory ESG Disclosurewith Voluntary ESG Disclosure being the lowest and Mandatory ESG Disclosure being the highest.

C. Voluntary ESG Disclosure Requirements

1. VARA may issue non-binding Guidance setting out ‘best practice standards’ regarding the conduct of specified VASPs or classes of VASPs in respect of ESG issues. Such ‘best practice

standards' could include considerations of sustainability that are consistent with such Entities' investment management strategies (if applicable), and diversity and inclusion practices within a VASP.

2. VASPs who comply with the Voluntary ESG Disclosure requirements understand that any compliance with the Guidance issued in accordance with Rule V.C.1 of this Company Rulebook is voluntary, though encouraged. However, VARA may require relevant VASPs to provide transparency into their ESG practices on a Compliance ESG Disclosure basis.

D. Compliance ESG Disclosure Requirements

1. VASPs required to comply with a Compliance ESG Disclosure level will be required to explain their ESG strategies in the UAE (including but not limited to investment or operational strategies relating to Virtual Asset mining or staking) or otherwise provide relevant information, for the purpose of increasing transparency into a VASP's ESG practices.
2. VARA may require VASPs to make their ESG strategies or relevant information public and/or otherwise made available to Virtual Asset market participants.

E. Mandatory ESG Disclosure Requirements

1. VASPs required to comply with a Mandatory ESG Disclosure level must, establish practices and procedures to raise awareness of ESG-related activities and opportunities including providing relevant information on their websites and/or social media sites.
2. VASPs which are required to comply with a Mandatory ESG Disclosure level must publish an annual ESG report which shall disclose, at a minimum—
 - a. governance policies, metrics and targets relating to how the VASP identifies, assesses, and manages risks and opportunities relating to sustainability, diversity and inclusion;
 - b. details on how material risks and opportunities relating to sustainability, diversity and inclusion are factored into the VASP's overall business strategies and VA Activity processes, including, where relevant, the data and/or methodologies used in identifying investments (whether or not denominated in Virtual Assets) and talent; and
 - c. factual summaries on the environmental and climate-related impact of data-intensive activities in the Virtual Asset sector.
3. VASPs which are required to comply with a Mandatory ESG Disclosure level shall make publicly available, in a prominent place on their website, up-to-date information related to the diversity and inclusion initiatives undertaken by such VASPs.

F. Virtual Asset Mining and Data-Intensive Activities

1. Notwithstanding a VASP's ESG disclosure level, all VASPs which have investments in Virtual Asset mining or staking businesses or conduct or facilitate Virtual Asset mining or staking activities (including by way of selling equipment) shall make publicly available in a prominent place on their website, up-to-date information related to—
 - a. the use of renewable and/or waste energy (e.g. hydroelectric energy, flared gas) by the VASP or its Group in the course of conducting Virtual Asset mining or staking activities (e.g. any renewable energy certificates purchased by the VASP and/or relevant Entities); and

- b. initiatives relating to decarbonisation (e.g. purchase of carbon offsets) and emission reduction of Virtual Asset mining or staking activities.

2. VARA may also require VASPs to provide the information referred to in Rule V.F.1 of this Company Rulebook in relation to other data-intensive activities.

G. Confidentiality

- 1. VARA shall maintain information presented in ESG reports, or other ESG disclosures, on a confidential basis, provided VARA may, in its sole discretion, publicly disclose information gathered in such ESG reports, or during such other requests, on an anonymous basis.
- 2. VASPs submitting ESG reports are deemed to consent to such anonymous, public disclosures, provided such disclosures are not required to be anonymous if they relate to an enforcement action commenced by VARA in accordance with the Regulations.

H. Service Providers to VASPs

- 1. When selecting service providers, VASPs should carefully consider the impact of their decision to contract with a service provider on all stakeholders. This includes taking into account the VASP's social and environmental responsibilities and whether the decision to contract with a service provider would have any negative impact on the VASP's ability to discharge such responsibilities.
- 2. With regard to service providers and, if applicable, their sub-contractors, VASPs should be satisfied that the service provider acts in an ethical and socially responsible manner and adheres to international standards on environmental protection and appropriate working conditions.

Part VI – Capital and Prudential Requirements

A. Application

- 1. VASPs shall comply with the Rules in this Part VI of the Company Rulebook ("Capital and Prudential Requirements").

B. Paid-Up Capital

- 1. VASPs shall, at all times, hold and maintain paid-up capital in the following amounts ("Paid-Up Capital")—

VA Activity	Paid-Up Capital Requirement
Advisory Services	AED 100,000.
Broker-Dealer Services	Broker-Dealer Services using a VASP Licensed by VARA to provide Custody Services or otherwise approved during the licensing process: the higher of (i) AED 400,000; or (ii) 15% of fixed annual overheads.
	In all other instances, the higher of (i) AED 600,000; or (ii) 25% of fixed annual overheads.
Category 1 VA Issuance	As specified in the VA Issuance Rulebook, or any Annex thereto.

Custody Services	The higher of (i) AED 600,000; or (ii) 25% of fixed annual overheads.
Exchange Services	Exchange Services using a VASP Licensed by VARA to provide Custody Services or otherwise approved during the licensing process: the higher of (i) AED 800,000; or (ii) 15% of fixed annual overheads.
	In all other instances, the higher of (i) AED 1,500,000; or (ii) 25% of fixed annual overheads
Lending and Borrowing Services	The higher of (i) AED 500,000; or (ii) 25% of fixed annual overheads.
VA Management and Investment Services	VA Management and Investment Services using a VASP Licensed by VARA to provide Custody Services or otherwise approved during the licensing process: the higher of (i) AED 280,000; or (ii) 15% of fixed annual overheads.
	In all other instances, the higher of (i) AED 500,000; or (ii) 25% of fixed annual overheads.
VA Transfer and Settlement Services	The higher of (i) AED 500,000; or (ii) 25% of fixed annual overheads.

2. Where a VASP is Licensed by VARA to carry out more than one VA Activity, the VASP must hold the amount of Paid-Up Capital specified in Rule VI.B.1 of this Company Rulebook for each VA Activity for which the VASP is Licensed. In such instances, the VASP shall calculate the Paid-Up Capital required for each VA Activity using the fixed annual overheads for that VA Activity only, provided that in combination all Paid-Up Capital is mutually exclusive and collectively exhaustive such that the total fixed annual overheads of the VASP are accounted for in aggregate. VASPs must reconcile Paid-Up Capital on a monthly basis.
3. Paid-Up Capital shall, at all times, be held and maintained in—
 - a. a trust account with a licensed bank in the UAE with VARA stated as the beneficiary;
 - b. a surety bond furnished by a surety company authorised to conduct business in the UAE, which shall have no end date and state VARA as a beneficiary; or
 - c. any other manner as may be specified by VARA upon granting a Licence.

C. Net Liquid Assets

1. VASPs shall at all times hold and maintain sufficient current liquid assets such that their surplus over current liabilities is worth at least 1.2 times their monthly operating expenses (“**Net Liquid Assets**”) as represented by the following calculation—

$$\text{Net Liquid Assets} \geq 1.2 \times \text{monthly operating expenses}$$

2. When calculating their Net Liquid Assets under Rule VI.C.1 of this Company Rulebook, VASPs must include such portion of their Operational Exposure to Virtual Assets (as agreed with VARA as a condition of their Licence) in their current liabilities, for the purposes of calculating their current liabilities.
3. Net Liquid Assets shall be reconciled on a daily basis and reported to VARA monthly.

4. Net Liquid Assets may be maintained in the following assets only—
 - a. cash and cash equivalents, as defined in internationally recognised accounting standards; and
 - b. Virtual Assets referencing USD or AED, as approved by VARA.

D. Insurance

1. VASPs must hold and maintain the following types of insurance adequate to the size and complexity of the business and VA Activities and in the manner specified by VARA in its Licence (“**Insurance**”)—
 - a. professional indemnity insurance;
 - b. directors’ and officers’ insurance;
 - c. commercial crime insurance or similar types of insurance for all Virtual Assets stored in hot wallets; and
 - d. any other type of insurance as assessed by VARA to be appropriate for a VASP’s business and VA Activities and stipulated in the conditions to its Licence.
2. All Insurance must be held and maintained with a regulated insurer.
3. Insurance may be held in the name of another Entity in the VASP’s Group, provided that the relevant policy—
 - a. explicitly states the VASP as an insured party; and
 - b. states the level of cover applicable to the VASP.
4. VARA may apply discretion during the licensing process if, for proven and demonstrated reasons the requirements in Rule VI.D.1 of this Company Rulebook cannot be met, provided that VASPs shall be required to protect against the risks that such Insurance is designed to cover through other means which will be specified by VARA as a condition of a Licence.

E. Reserve Assets

1. VASPs shall, at all times, maintain reserve assets equivalent to one hundred percent (100%) of the liabilities owed to clients with respect to all VA Activities (“**Reserve Assets**”).
2. VASPs must hold Reserve Assets on a one-to-one basis in the same Virtual Asset that liabilities are owed to its clients.
3. Reserve Assets must be reconciled on a daily basis and audited by an independent third-party auditor no less than every six (6) months. VASPs shall include such audit reports as part of the subsequent quarterly report to VARA required in the Compliance and Risk Management Rulebook.

F. Notifications and other Requirements

1. VASPs shall notify VARA immediately if, at any time, it is unable to maintain or fails to meet the Paid-Up Capital, Net Liquid Assets, Insurance or Reserve Assets requirements above and such

notification shall include details of—

- a. all deficit amounts;
- b. the causes of the failure;
- c. remedial actions that have been, and will be, taken to rectify the breach; and
- d. the expected timeline for such remedial actions to be completed.

2. VASPs shall provide updates to VARA on a daily basis in respect of any notification under Rule VI.F.1 of this Company Rulebook above, unless otherwise directed by VARA or until the VASP confirms and VARA is satisfied that it has rectified all failures and is in compliance with all requirements.
3. Notwithstanding all other requirements in the Compliance and Risk Management Rulebook, VASPs shall establish and maintain clear procedures to monitor and identify all sources of risks or potential risks that may impact its operation and shall consider the potential adverse impact of such risks on its level of Paid-Up Capital, Net Liquid Assets, Insurance or Reserve Assets.
4. VARA may require VASPs to hold and maintain additional Paid-Up Capital, Net Liquid Assets, Insurance or Reserve Assets based on the size, scope, geographic exposure, complexity and nature of the VA Activities and operations of a VASP.

Part VII – Insolvency and Wind Down

Introduction

The purpose of this Part VII is to provide for the safeguarding and stable operations of Virtual Asset markets by introducing procedures for:

- a VASP that elects to discontinue its business or operations; and
- a VASP that is Insolvent or subject to Insolvency Proceedings.

A. Wind Down Plan

1. All VASPs shall have and maintain a wind down plan (“**Wind Down Plan**”), which shall include the following—
 - a. processes for identifying and mitigating any material risk or obstacles to winding down in an orderly and timely manner;
 - b. an evaluation of the resources that are needed to facilitate an orderly and timely wind down;
 - c. internal controls and procedures to ensure the safekeeping and prompt onward transferring of clients’ Virtual Assets (including returning Virtual Assets to clients);
 - d. personnel management and exit arrangements;
 - e. communications strategy (including the provision of clear and timely disclosures to all clients);
 - f. knowledge transfer as required to support migration of VA Activities and all relevant operations to alternate VASPs;
 - g. system redundancies and retention of records;
 - h. continue to maintain a surety bond until completion of the wind down process;
 - i. discontinue taking on new clients;

- j. identify and itemise all current and contingent liabilities;
- k. ensure that the sale of Client Money and/or Client VAs is explicitly excluded from, and not necessary for, implementing or completing the Wind Down Plan, or any other plan, procedures or scheme directed by an Insolvency Appointee, or the sale of the VASP's assets or business as a going concern; and
- l. ensure VARA has the power and ability to intervene and/or assume the direction and/or control of Client Money and/or Client VAs at VARA's election, including but not limited to where the VASP is in breach of any Regulation, Rule or Directive.

2. In the event that a VASP elects to discontinue its business or operations where it is not Insolvent or subject to Insolvency Proceedings, the VASP must—

- a. notify VARA not later than one (1) day after such decision;
- b. provide VARA its latest up-to-date Wind Down Plan at the time of such notification;
- c. implement the Wind Down Plan, subject to any amendments or additions notified to it by VARA;
- d. make any further changes notified to it by VARA at any stage throughout the implementation and completion of the Wind Down Plan; and
- e. report to VARA every week throughout the implementation and completion of the Wind Down Plan; and
- f. provide all other updates and/or reports as requested by VARA at any time.

B. Insolvency

1. In the event a VASP is subject to Insolvency Proceedings, the VASP shall co-operate fully with the Insolvency Appointee to implement the Wind Down Plan as set out in Rule VII.A.1 of this Company Rulebook, or any other plan, procedures or scheme as the Insolvency Appointee deems to be commensurate with the duties and obligations imposed by the relevant Insolvency Proceedings.

Part VIII – Material Change to Business or Control

A. No Material Change

1. VASPs shall obtain VARA's written approval prior to—

- a. facilitating any development or occurrence of Material Change to themselves; or
- b. entering into any business or conducting any VA Activity, directly or indirectly, except for those business(es) and VA Activity(ies) in which the VASP and its Subsidiaries are engaged on the date of the Licence being granted and authorised by VARA.

2. VASPs shall not create, incur, assume, permit to exist or otherwise become liable with respect to any debt that could be reasonably expected to cause a Material Change.

3. VASPs shall not cause any occurrence of a Material Change. In the event that the acquisition or disposal by a VASP could reasonably be expected to cause a Material Change, such VASP shall immediately cease the acquisition or disposal.

4. Without obtaining VARA's prior written approval, VASPs may not implement any changes to its VA Activities authorised under the Licence, including the—

- a. addition of any VA Activity; or
- b. material modification of the scope of any VA Activity.

5. VASPs shall ensure that any change in their business plan covering internal controls, organisational structure, contingency plans and related matters could not be reasonably expected to cause a Material Change.
6. VASPs shall ensure that any change under Rules VIII.A.1-5 of this Company Rulebook in aggregate could not reasonably be expected to cause a Material Change.

B. Cessation of Business

1. VARA may revoke or suspend a Licence (in relation to all or certain VA Activities), if a VASP does not—
 - a. carry out all or some of the VA Activities authorised under the Licence for an extended period; and
 - b. notify VARA of its plan to reinstate or carry out relevant VA Activities.
2. In the event that a VASP intends to cease to carry out any VA Activities authorised under its Licence, it shall notify VARA and request a revocation of either—
 - a. in the event that all VA Activities authorised under a Licence are to be ceased, the Licence; or
 - b. in the event that only some of the VA Activities authorised under a Licence are to be ceased, the VA Activities to be ceased.
3. VASPs shall notify VARA as soon as reasonably practicable and in any event not later than thirty (30) Working Days before such intended cessation.

C. Change of Control

1. No action shall be taken, except with the prior written approval of VARA, that may result in a change of Control of a VASP.
2. Prior to any change of Control, the VASP, together with the Entity seeking to acquire Control of the VASP, shall submit a written application to VARA in a form and substance acceptable to VARA, including but not limited to detailed information about the Entity.
3. VARA may determine upon application that any Entity does not, or upon the taking of some proposed action will not, Control another Entity. Such determination shall be made within thirty (30) Working Days or such further period as VARA may prescribe. The filing of an application pursuant to this Part VIII of the Company Rulebook in good faith by any Entity shall relieve the applicant from any obligation or liability imposed by this Part VIII of the Company Rulebook with respect to the subject of the application until VARA has acted upon the application. VARA may revoke or modify its determination whenever, in its sole and absolute discretion, revocation or modification is consistent with this Part VIII of the Company Rulebook. VARA may consider the following factors in making such a determination—
 - a. whether such Entity's purchase of shares is made solely for investment purposes and not to acquire Control over the VASP;

- b. whether such Entity could direct the Board or Staff, or otherwise influence the policies of the VASP;
- c. whether such Entity could propose directors in opposition to nominees made by the shareholders of the VASP;
- d. whether such Entity could solicit or participate in soliciting proxy votes with respect to any matter presented to the shareholders of the VASP; or
- e. any other factor that indicates such Entity would or would not exercise Control of the VASP.

4. VARA shall approve or deny every application for a change of Control of a VASP hereunder within thirty (30) Working Days from the filing of an application deemed by VARA to be complete. Such period of thirty (30) Working Days may be extended by VARA, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part VIII of the Company Rulebook.

5. In determining whether to approve a proposed change of Control, VARA shall, among other factors, take into consideration the public interest and the needs and convenience of the public in the Emirate.

D. Mergers and Acquisitions

- 1. No action shall be taken, except with the prior written approval of VARA, that may result in a merger or acquisition of all or a substantial part of the assets of a VASP.
- 2. Prior to any such merger or acquisition, an application containing a written plan of merger or acquisition shall be submitted to VARA by the Entities that are to merge or by the acquiring Entity, as applicable. Such plan shall be in form and substance satisfactory to VARA, and shall specify each Entity to be merged, the surviving Entity, or the Entity acquiring all or substantially all of the assets of the VASP, as applicable, and shall describe the terms and conditions of the merger or acquisition and the mode of carrying it into effect.
- 3. VARA shall approve or deny a proposed merger or a proposed acquisition of all or a substantial part of the assets of a VASP within thirty (30) Working Days after the filing of an application that contains a written plan of merger or acquisition and is deemed by VARA to be complete. Such period of thirty (30) Working Days may be extended by VARA, for such additional reasonable period of time as may be required to enable compliance with the requirements and conditions of this Part VIII of the Company Rulebook.
- 4. In determining whether to approve a proposed merger or acquisition, VARA shall, among other factors, take into consideration the public interest and the needs and convenience of the public in the Emirate.

Schedule 1 – Definitions

Term	Definition
“Advisory Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Board”	means the board of directors of a VASP.
“Broker-Dealer Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Capital and Prudential Requirements”	has the meaning ascribed to it in Rule <u>VI.A.1</u> of this Company Rulebook.
“Category 1 VA Issuance”	has the meaning ascribed to it in the VA Issuance Rulebook.
“CBUAE”	means the Central Bank of the United Arab Emirates.

“Chief Information Security Officer” or “CISO”	has the meaning ascribed to it in the Technology and Information Rulebook.
“Client Money”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Client VA”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Company Rulebook”	means this Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Company Secretary”	has the meaning ascribed to it in Rule <u>I.E.1</u> of this Company Rulebook.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance ESG Disclosure”	means the compliance ESG disclosure level defined in <u>Part V</u> of this Company Rulebook.
“Compliance Officer” or “CO”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Control”	<p>means the possession, directly or indirectly (including but not limited to by way of acting jointly or in concert with one or more Entities), of the power to influence, direct or cause the direction of the management and policies of a VASP whether through the ownership of shares of such VASP, the shares of any Entity that possesses such power, or any other means.</p> <p>Control shall be presumed to exist if an Entity, directly or indirectly (including but not limited to by way of acting jointly or in concert with one or more Entities), owns, controls, or holds with power to vote with twenty-five percent (25%) or more of the voting shares of a VASP or of any Entity that owns, controls, or holds with power to vote with twenty-five percent (25%) or more of the voting shares of such VASP, or who have the right to appoint or dismiss the majority of the Board or Senior Management. No Entity shall be deemed to control another Entity solely by reason of them being an officer or director of such other Entity.</p>
“Controlling Entity”	means an Entity which has Control over a VASP.
“Critical or Important Function”	<p>means a Function whose discontinued or defective performance would materially impair—</p> <ul style="list-style-type: none"> [a] the continuing compliance of a VASP with the conditions and obligations of its Licence; [b] its compliance with its other legal obligations; [c] its financial performance; or [d] the soundness or continuity of its core business activities.
“Custody Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Data Protection Officer” or “DPO”	has the meaning ascribed to it in the Technology and Information Rulebook.
“Decentralised Autonomous Organisation” or “DAO”	means, generally, any organisation autonomously governed or otherwise managed by a decentralised network, group or collection of Entities, by way of public or private voting mechanisms, whether utilising Distributed Ledger Technology or other means.

“Directive”	has the meaning ascribed to it in the Regulations.
“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to it in the Dubai VA Law.
“Dubai VA Law”	means <i>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</i> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“ESG”	means environmental, social and governance.
“Exchange Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Fit and Proper Person”	means an individual who complies with all fit and proper requirements in <u>Part III</u> of this Company Rulebook.
“Function”	means a service, process, activity or role.
“Group”	means a VASP and any Entity under the same Control with the VASP.
“Guidance”	has the meaning ascribed to it in the Regulations.
“Insolvency Appointee”	means a liquidator, receiver, administrator, compulsory manager, trustee or similar officer appointed in respect of an Entity or its assets.
“Insolvency Proceedings”	has the meaning ascribed to it in the Regulations.
“Insolvent”	has the meaning ascribed to it in the Regulations.
“Insurance”	has the meaning ascribed to it in Rule <u>VI.D.1</u> of this Company Rulebook.
“Lending and Borrowing Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Mandatory ESG Disclosure”	means the mandatory ESG disclosure level defined in <u>Part V</u> of this Company Rulebook.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Material Change”	means a change in, or relating to, a VASP with respect to its business and operations (including its VA Activities) and its Group which, taken as a whole, could reasonably be expected to have a significant effect on the VASP’s business model, operations, VA Activities, and/or ability to comply with all applicable laws and regulatory requirements.
“Material Outsourcing”	is an Outsourcing that includes a Function that is a Critical or Important Function.
“Money Laundering Reporting Officer” or “MLRO”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Net Liquid Assets”	has the meaning ascribed to it in Rule <u>VI.C.1</u> of this Company Rulebook.
“Operational Exposure”	means an amount representing the value of Virtual Assets at risk of loss, dissipation, devaluation or inaccessibility in the event of

	operational, procedural, counterparty, settlement or other failure experienced by the VASP.
“Outsourcing”	means an arrangement where a Service Provider performs a process, service or activity on behalf of a firm which the firm would otherwise carry out itself on a recurrent or ongoing basis. It is intended to include only those services that were or can be delivered by internal Staff and management, and may include both regulated and unregulated Functions.
“Outsourcing Policy”	has the meaning ascribed to it in Rule <u>IV.C.1</u> of this Company Rulebook.
“Paid-Up Capital”	has the meaning ascribed to it in Rule <u>VI.B.1</u> of this Company Rulebook.
“PDPL”	means the <i>Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data</i> .
“Personal Data”	has the meaning ascribed to it in the PDPL.
“Politically Exposed Person”	has the meaning ascribed to it in <i>Cabinet Decision No. (10) of 2019 Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations</i> , as may be amended from time to time.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Related Party”	means the chairman of the Board, members of the Board, members of the Senior Management, Staff and the companies in which any of such Entities owns ten percent (10%) or more of its share capital or other ownership interest, as well as the Subsidiaries or affiliate companies of such companies.
“Reserve Assets”	has the meaning ascribed to it in Rule <u>VI.E.1</u> of this Company Rulebook.
“Responsible Individuals”	has the meaning ascribed to it in Rule <u>I.C.1</u> of this Company Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	means the executive management of a VASP responsible and accountable to the Board for the sound and prudent day-to-day management of the VASP, generally including but not limited to, the chief executive officer, chief financial officer, chief risk officer, and heads of the compliance and internal audit functions, or as equivalent roles may be titled.
“Service Provider”	means an Entity that contracts with a VASP for the provision of any aspect of the VASP’s functions. The Service Provider may be within or outside the Emirate and may be an independent third party or an Entity related to the VASP.
“Staff”	means all individuals working for a VASP including the members of the Senior Management but excluding members of the Board. If an individual is both a member of the Senior Management and a member of the Board, then such individual is also considered as Staff.

“Subsidiary”	means a company of which an Entity, or such Entity’s Subsidiary(ies), own(s) directly or indirectly more than fifty percent (50%) of the voting capital or similar right of ownership.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“UAE”	means the United Arab Emirates.
“Ultimate Beneficial Owner” or “UBO”	means— [a] individuals who ultimately own or have Control; or [b] if no individual satisfies (a) above, then an individual with the highest position in Senior Management.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VA Issuance Rulebook”	means the Virtual Asset Issuance Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“VA Management and Investment Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“VA Transfer and Settlement Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity Licensed by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.
“Voluntary ESG Disclosure”	means the voluntary ESG disclosure level defined in <u>Part V</u> of this Company Rulebook.
“Wind Down Plan”	has the meaning ascribed to it in Rule <u>VII.A.1</u> of this Company Rulebook.
“Working Day”	means any day which is not a weekend or public holiday in the Emirate.

Compliance and Risk Management Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Compliance and Risk Management Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out any VA Activity in the Emirate.

This Compliance and Risk Management Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out any

VA Activity must also comply with the following Rulebooks applicable to all VASPs—

- Company Rulebook;
- Technology and Information Rulebook;
- Market Conduct Rulebook; and
- All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

Capitalised terms in this Compliance and Risk Management Rulebook have the meanings ascribed to them in the Regulations or as otherwise defined herein or provided in Schedule 1.

Unless otherwise stated, all requirements in this Compliance and Risk Management Rulebook are Rules and have binding effect.

Part I – Compliance Management

Introduction

Part I of this Compliance and Risk Management Rulebook sets out—

- general principles for regulatory compliance;
- the implementation of a compliance management system including appointing a Compliance Officer (“CO”);
- management, operations and information risk;
- record keeping and audit; and
- employee management and training.

A. General Principles

VASPs shall comply with the spirit of the following principles when conducting all their business from or through, or servicing the Emirate, including all VA Activities.

1. *Integrity – honesty and fairness*: VASPs should act truthfully, justly and equitably, in good faith serving the best interests of their clients, yet at all times preserving market integrity.
2. *Diligence*: VASPs should act with due skill, care and diligence reasonably expected of a VASP of a similar nature and/or catering to a similar activity.
3. *Capabilities*: VASPs should have, and effectively employ necessary resources (financial, technical or otherwise) and procedures for the sound, effective and efficient operation of their business, including VA Activities.
4. *Client assets*: VASPs should ensure that client assets are promptly and properly accounted for, and adequately safeguarded.
5. *Effective disclosures*: VASPs should ensure that any disclosure is clear, concise and effective, and contains information necessary for their clients to make an informed decision and be kept up-to-date. VASPs should dispatch information in a timely manner if ongoing disclosure is required by relevant authorities, including VARA, or under any fiduciary duty owed by VASPs to their clients.
6. *Compliance*: VASPs should devise effective strategies to ensure ongoing compliance with—

- a. all legal and regulatory requirements (including any conditions in respect of a Licence) applicable to the conduct of their business, including VA Activities; and
- b. their own constitutional documents, internal policies and controls, so as to promote the best interests of their clients and for promoting the integrity of the market.

7. *Dealings with regulators.* VASPs should act in an open and transparent manner with regulators at all times, including VARA.

B. Compliance Management System

1. VASPs shall establish and maintain an effective compliance management system (“**CMS**”) which—
 - a. covers all relevant aspects of their operations, including the unfettered access to necessary records and documentation by the Board and relevant Staff;
 - b. is independent of all operational and business functions;
 - c. ensures that the CO is notified of any material non-compliance promptly;
 - d. comprises technical competence, resources (including financial and non-financial) and experience necessary for the performance of their functions; and
 - e. comprises a testing and monitoring programme that is risk-based and designed to regularly select and review different areas of the business and analyse key performance and risk indicators,in order to allow them to identify potential compliance violations and to ensure that they comply with all applicable laws and regulatory requirements, and their own internal policies and procedures at all times.
2. The CO shall ultimately be responsible for establishing and administering the CMS, and notifying VARA and other relevant authorities of the occurrence of any material non-compliance by the VASP, its Board or its Staff with applicable legal and regulatory requirements.
3. VASPs shall establish, maintain and enforce clear and detailed compliance policies and procedures to enable all Staff and the Board to—
 - a. comply with all applicable legal and regulatory requirements at all times, including all conditions in respect of a Licence, record keeping, business practices, AML/CFT, and compliance with relevant client, proprietary and Staff dealing requirements;
 - b. ensure that client complaints are handled properly with appropriate remedial action. Complaints should be handled and investigated by Staff who are not directly involved in the subject matter of the complaint; and
 - c. have access to all necessary information required to perform a business transaction.
4. The CMS and the compliance policies and procedures shall be reviewed and updated from time to time to ensure that they are aligned with the changing business and regulatory landscape applicable to the global Virtual Asset sector.
5. VASPs shall ensure that all Staff performing compliance functions are Fit and Proper Persons and possess the necessary skills, qualifications and experience for their roles.
6. To the extent that VASPs carry out any VA Activities or similar business activities anywhere other than the Emirate, VASPs shall comply with all applicable laws and regulatory requirements in any jurisdiction in which they carry out such VA Activities or similar business activities.

C. Duties of the Compliance Officer

1. VASPs shall appoint a CO who—
 - a. possesses at least five (5) years of relevant experience in a compliance function;
 - b. is a Fit and Proper Person as approved by VARA;
 - c. is a resident in the UAE or holds a UAE passport;
 - d. is a full-time employee of the VASP; and
 - e. reports directly to the Board.

Such appointment shall be reviewed annually to ensure that the CO remains a Fit and Proper Person capable of discharging all relevant duties. VARA has the sole discretion to request a VASP to provide such evidence as VARA may require which shows that the above requirements are satisfied.
2. The CO shall be responsible for—
 - a. ensuring Staff, including Senior Management, are properly and adequately trained in respect of their understanding and compliance with all applicable laws and regulatory requirements, including those relating to consumer protection and AML/CFT;
 - b. developing and implementing compliance policies and procedures, including a Business Continuity and Disaster Recovery Plan (“**BCDR Plan**”) as required in the Technology and Information Rulebook;
 - c. assessing emerging issues and risks;
 - d. reporting compliance activities and compliance audits to the Board; and
 - e. if necessary, ensuring appropriate corrective actions are taken in response to deficiencies in the CMS and/or non-compliance with any applicable laws or regulatory requirements.
3. Compliance activities may be delegated to appropriate professionals, provided that—
 - a. the CO shall continue to be held accountable for all responsibilities and obligations in relation to the implementation of the CMS; and
 - b. all applicable requirements in the Company Rulebook, including Outsourcing management requirements, are complied with.
4. Subject to relevant requirements in the Company Rulebook and if deemed appropriate by the VASP, the CO may hold more than one (1) non-client facing role within the VASP, provided such roles do not create conflicting duties, including but not limited to, the Money Laundering Reporting Officer (“**MLRO**”) and the head of the risk function. VARA will take into account other roles held by the CO in determining whether the individual is a Fit and Proper Person.

D. Risk Management

1. VASPs shall establish and maintain—
 - a. an effective risk management function;
 - b. policies and procedures; and
 - c. risk measurement and reporting methodologies,

each commensurate with the nature, size, complexity, and risk profile of the VASP in order to identify, measure, quantify, manage and monitor the risks, whether financial, technological or otherwise, to which they are or may be exposed. Such policies and procedures should be followed strictly to ensure that risks are maintained at acceptable and appropriate levels.

2. The risk management function should consist of a sufficient number of suitably qualified and experienced Staff. The head of the risk function of a VASP must have the appropriate qualifications and authority to oversee and monitor the overall risk exposures of the VASP. The CO may also be the head of the risk function. If the head of the risk function is a separate individual from the CO, the head of the risk function must also report directly to the Board of the VASP.
3. The Board shall ensure that the risk management policies are subject to ongoing comprehensive review, particularly when there is a material change in the VASP's business, operations or Senior Management or Staff, or to the market conditions and applicable laws and regulations that may affect the risk exposure of the VASP.
4. The head of the risk function of a VASP shall submit risk exposure reports to the Board which identify and report all actual or potential risks. Such reports must be submitted to the Board at least once every quarter, or more frequently if required for the VASP to address a specific risk which has been identified.
5. The effectiveness of the risk management policy of each VASP will depend on the types of risks associated with the VASP and its business operations, including the VA Activities it carries out. The key types of risks that must be considered by all VASPs, and reported in the risk exposure reports under Rule I.D.4 of this Compliance and Risk Management Rulebook above, to the extent they are applicable, and the mitigating measures which must be adopted for each type of risk include, but are not limited to—
 - a. Financial stability risks.
 - i. *Financial soundness:* Risks arising when a VASP lacks the necessary capital, liquidity or reserves to run operations (both in the going-concern and wind-down scenario) and meet all commitments to its clients, including but not limited to when a VASP is likely to be unable to comply with any of its Capital and Prudential Requirements in the Company Rulebook.
 - ii. *Market risk:* Risks arising from the type and nature of market risk undertaken by the VASP (e.g. the nature of market risk exposure of the VASP's services and VA Activities). In relation to such risks, VASPs shall adopt mitigating measures including but not limited to—
 1. regular control techniques to monitor market risks, including conducting regular reviews of financial statements and the value of their Virtual Asset holdings; and
 2. establish and maintain effective risk management measures to quantify the impact of changing market conditions on themselves and their clients. Factors to be considered include—
 - (a) unspecified adverse market movements (including but not limited to 'flash crashes', catastrophic risk or tail events), by using an appropriate value-at-risk model or other methodology to estimate potential loss;
 - (b) individual market factors, to measure the sensitivity of the VASP's risk exposure to specific market risk factors; and
 - (c) stress testing, determining the effect of material changes in market conditions (whether or not specific to Virtual Asset markets) on the VASP

using quantitative and qualitative variable assumptions.

- iii. *Credit risks:* Risks arising from the type and nature of credit risk undertaken by the VASP (e.g. the nature and level of credit risk exposure of the VASP's services and VA Activities). In relation to such risks, VASPs shall adopt mitigating measures, at both an individual account and consolidated account level, including but not limited to—
 - 1. establish and maintain an effective credit rating system to evaluate the creditworthiness of their clients and counterparties;
 - 2. adopt clearly defined objective measures to evaluate potential clients and counterparties and to determine or review the relevant credit ratings which are used to set appropriate credit, trading and position limits for all clients and counterparties, which shall be enforced at all times;
 - 3. use appropriate quantitative risk measurement methodologies to effectively calculate and monitor the credit exposure of VASP in relation to clients and counterparties, including pre-settlement credit exposures and settlement risks. Credit risks posed by all clients and counterparties belonging to the same group of Entities can be aggregated for the purpose of measuring the credit exposure of the VASP;
 - 4. if applicable in respect of the VA Activities of the VASP, establish and maintain all policies in respect of margin required under any Rulebook, which notwithstanding all other requirements in those Rulebooks should include—
 - (a) the types of margin which may be called, the applicable margin rates and the method of calculating the margin;
 - (b) the acceptable methods of margin payment and forms of collateral;
 - (c) the circumstances under which a client or counterparty may be required to provide margin and additional margin, and the consequences of a failure to meet a margin call, including the actions which the VASP may be entitled to take; and
 - (d) applicable escalation procedures where a client or counterparty fails to meet successive margin calls.
- iv. *Liquidity risks:* Risks arising from the type and nature of the VASP's liquidity or asset and liability mix. In relation to such risks, VASPs shall adopt mitigating measures including but not limited to—
 - 1. enforce concentration limits with respect to particular products, markets and counterparties, taking into account their liquidity profile and the liquidity profile of the VASP;
 - 2. regularly monitor any maturity mismatch between sources and funding requirements and concentrations of individual Virtual Assets, markets and counterparties; and
 - 3. establish clear default procedures to alert relevant Staff and Senior Management to potential liquidity problems and to provide such Staff and Senior Management with sufficient time to minimise the impact brought by any client's or counterparty's liquidity issues.

b. Market conduct risks.

- i. *Business strategy*: Risks arising from the overall strategy and current sources of business of the VASP (e.g. strategic planning process and achievability of strategy).
- ii. *Client onboarding risks*: Risks arising from onboarding clients (individuals and corporates). This refers to the level of client due diligence (“**CDD**”) applied, such as sanction screening, risk rating and watchlist screening.
- iii. *Organisation and regulation*: Risks arising from the structure of a VASP, the characteristics and nature of responsibilities of UBOs, Board members and Senior Management responsibilities.
- iv. *Operational risks*: Risks arising from type and nature of operational risk involved in the VASP’s activities (e.g. direct or indirect loss from inadequate or failed internal processes, systems or external events).
- v. *Quality of management & corporate governance*: Risks arising from the quality of the VASP’s management, the nature of the corporate governance, management information and compliance culture, including but not limited to non-compliance with relevant requirements in the Company Rulebook.
- vi. *Relationship with regulators*: Risk arising from the nature of the VASP’s relationship with other regulators, including recent regulatory history.
- vii. *Cybersecurity risks*: Risks of exposure or loss from a cyber-attack, data, system or security breach, including any breach of Personal Data security, not limited to non-compliance with relevant requirements in the Technology and Information Rulebook. VASPs must also include all risks relating to the VASP’s reputation in such events.

c. Compliance and risk management risks.

- i. *AML/CFT, market abuse & fraud*: Risks arising from the VASP’s susceptibility to financial crime risk arising from money laundering, market abuse, terrorism financing, and fraud, including but not limited to non-compliance with relevant requirements in this Compliance and Risk Management Rulebook.
- ii. *Outsourcing & counterparty risks*: Risks arising from Outsourcing to third parties, developing relationships or dependencies on counterparties in any transactions, including with any Controlling Entity, Group Entity or UBO.
- iii. *Risk management systems*: Risks arising from the nature and effectiveness of the systems and procedures to identify, measure, monitor and control the VASP’s risks (e.g. credit risk, insurance underwriting risk, market risk, operational risk, legal risk and new product risk).
- iv. *Compliance function and arrangements*: Risks arising from the nature and effectiveness of the compliance function of a VASP. These include its mandate, structure, staffing, methodology, reporting lines and effectiveness.
- v. *Business continuity*: risks arising from the effectiveness of business continuity arrangements, including but not limited to non-compliance with relevant requirements in this Compliance and Risk Management Rulebook.

d. Consumer protection risks.

- i. *Communications with clients & financial promotions*: Risks arising from the nature of financial promotion and advertising practices employed by the VASP, including but not limited to non-compliance with relevant requirements in the Market Conduct Rulebook.
- ii. *Legal risks*: Risks arising from the nature of the VASP’s contractual agreements.
- iii. *Disclosure and reporting*: Risks arising from the nature of terms of business, periodic statements and other documentation provided to clients, including but not limited to

non-compliance with relevant requirements in the Market Conduct Rulebook.

iv. *Client assets*: Risk arising from the VASP holding or controlling of Client Money and Client VAs.

E. Operation Management

1. VASPs shall establish and maintain effective operational policies and processes to ensure—
 - a. they have regular exchange of information with their clients, Group and, where appropriate, counterparties;
 - b. the integrity of their dealing practices, including the treatment of all clients in a fair, honest and professional manner;
 - c. the safeguarding of both their assets and all Virtual Assets (including Client VAs) in accordance with applicable requirements in this Compliance and Risk Management Rulebook and the Technology and Information Rulebook;
 - d. the maintenance of proper records and the reliability of the information contained in such records in accordance with applicable requirements in this Compliance and Risk Management Rulebook; and
 - e. the compliance by VASP and all its Staff with all applicable laws and regulatory requirements.
2. Where a VASP may act on behalf of the client in relation to the operation of an account, it shall properly communicate to the client the necessary procedures and terms and conditions under which the VASP may act on its behalf in transactions which are consistent with the stated objectives of the client and strictly follow such procedures.
3. In addition to applicable requirements in the Market Conduct Rulebook, VASPs shall establish and enforce procedures to ensure that there are safeguards against any of their Staff or members of the Board taking advantage of confidential information or Inside Information.
4. In addition to applicable requirements in the Technology and Information Rulebook, VASPs shall establish and maintain robust procedures to protect their Virtual Assets and Client VAs from theft, fraud and/or misappropriation. All Staff and members of the Board should follow all applicable internal protocols to acquire, transfer or otherwise dispose of any of the VASP's Virtual Assets and Client VAs in accordance with applicable requirements in this Compliance and Risk Management Rulebook and the Technology and Information Rulebook.
5. VASPs shall regularly check all—
 - a. records and reports, whether issued by third parties, such as banks, other VASPs, or other virtual asset service providers outside of the Emirate; and
 - b. relevant information recorded on all systems including distributed ledgers, and reconcile the above with their internal records for the purpose of identifying any errors, omissions or misplacement of assets, including Virtual Assets.
6. VASPs may establish committees as they deem appropriate in order to ensure compliance with all applicable laws and regulatory requirements. VARA may require a VASP, either as a condition of granting a Licence or at any stage thereafter, to establish any committee(s) determined by VARA as it deems appropriate, and VASPs shall comply with such requirements.

F. Books and Records

1. VASPs shall keep their books and records properly in their original form or native file format (including as recorded on distributed ledgers where appropriate), including—
 - a. keeping proper audit trails of all transactions, such as the amount, date and time of each transaction, any payment instruction, the total amount of fees and charges, the names, details of accounts or VA Wallets and country of residence of the clients and to the extent practicable, that of any other Entities involved in the transaction, so as to enable the VASP to carry out thorough investigation of any Suspicious Transactions (subject to further requirements set out in Part III of this Compliance and Risk Management Rulebook);
 - b. maintaining and organising all information relating to clients produced by third parties;
 - c. maintaining sufficient records to prove that the VASP is in compliance with all applicable laws and regulatory requirements, including AML/CFT laws and requirements in Part III of this Compliance and Risk Management Rulebook;
 - d. keeping proper records to enable the VASP to carry out an audit in a convenient manner;
 - e. keeping a general ledger containing all assets (including Virtual Assets), liabilities, ownership equity, income and expense accounts;
 - f. keeping statements or valuations sent or provided to clients and counterparties;
 - g. keeping minutes of meetings of the Board;
 - h. retaining communications and documentation related to investigations of client complaints and transaction error resolution or concerning facts giving rise to potential violation of laws and regulatory requirements; and
 - i. maintaining a conflicts of interest register in accordance with the Company Rulebook.
2. VASPs shall retain each such record as set out in Rule I.F.1 of this Compliance and Risk Management Rulebook in accordance with the following timelines—
 - a. no less than eight (8) years; or
 - b. for an indefinite period for all records which may relate to national security of the UAE.
3. VASPs shall furnish copies of any records to VARA in accordance with all applicable requirements in the Regulations, Rules or Directives.

G. Audit

1. External audit.
 - a. VASPs shall appoint an independent third-party auditor to perform an audit of the financial statements of the VASP in order to make available an annual report, and promptly notify VARA of the full name and contact details of the auditor upon appointment.
 - b. The annual report of VASPs shall promptly be made available to their clients and VARA upon request.
 - c. VASPs should understand the steps taken by the auditor in proving the existence and ownership of Virtual Assets and ascertaining the reasonableness of the valuation of Virtual Assets.
 - d. The accounting information given in the annual report shall be prepared in accordance with generally accepted accounting principles.
 - e. If requested, VASPs shall procure relevant counterparties to cooperate with the auditor and to provide with the auditor all necessary information for the auditor to conduct the audit.

- f. VARA may in its sole and absolute discretion require a VASP to appoint alternative auditors if their original auditors are not deemed appropriate for the size and complexity of their business and in terms of reputation.

2. Internal audit.

- a. VASPs shall, where applicable, establish and maintain an objective internal audit function which shall be independent of the operational function and submit regular reports directly to the Senior Management.
- b. VASPs shall establish and maintain clear policies in defining the role and responsibilities of, and the working relationship between, the internal and external auditors.
- c. The internal audit function shall—
 - i. perform audit work regularly and at least on a quarterly basis;
 - ii. inform the Senior Management of findings and recommendations; and
 - iii. follow up with and resolve matters or risks highlighted in the relevant reports.

H. Regulatory Reporting

- 1. On a monthly basis, VASPs shall as a minimum submit to VARA the following information—
 - a. their balance sheet and a list of all off-balance sheet items;
 - b. their statement of profit and loss;
 - c. their income statement;
 - d. their cashflow statements;
 - e. addresses of their VA Wallets;
 - f. a full list of Entities in their Group that actively invest their own, or the Group's, portfolio in Virtual Assets, and a complete record of all transactions, including but not limited to loans or any transactions involving any VA Activity for which the VASP is Licensed, with all such Entities identified; and
 - g. transactions with Related Parties as prescribed in the Company Rulebook.
- 2. On a quarterly basis, VASPs shall as a minimum submit to VARA the following information—
 - a. the minutes of all Board meetings and Board committee meetings;
 - b. a statement demonstrating compliance with any financial requirements established by VARA including but not limited to Reserve Assets;
 - c. financial projections and strategic business plans; and
 - d. a risk exposure report prepared and submitted to the Board in accordance with Rule I.D.4 of this Compliance and Risk Management Rulebook.
- 3. On an annual basis, VASPs shall as a minimum submit to VARA the following information—
 - a. audited annual financial statements, together with an opinion and an attestation by an independent third-party auditor regarding the effectiveness of the VASP's internal control structure;
 - b. an assessment by Senior Management of the VASP's compliance with such applicable laws, Regulations, Rules and Directives during the fiscal year covered by the financial

statements;

- c. certification of the financial statements by a member of the Board or a Responsible Individual attesting to the truth and correctness of those statements;
- d. a representative sample of all documentation relating to client onboarding (including actual documentation of the first one hundred (100) clients onboarded of the year);
- e. descriptions of product offerings relating to their VA Activities;
- f. Group structure chart including shareholding of the VASP and the identity of all UBOs;
- g. the names of each of the members of the Board and the Senior Management in the VASP, a brief biography of each such member including their qualifications and experience and any position that a member of the Board or the Senior Management holds in other Entities;
- h. the identification of any independent director(s) if applicable;
- i. the names of all the members of any committees, the authorities and assignments entrusted thereto, and activities carried out by the committees during that year; and
- j. the number of meetings held by the Board and the committees, and the names of the attendees.

4. VARA may require upon request to a VASP, information to be provided in addition to those listed in Rule I.F.1 of this Compliance and Risk Management Rulebook.

I. Regulatory Notifications

1. VASPs shall notify VARA in writing of—
 - a. any changes to items set out in Rule I.H.3 of this Compliance and Risk Management Rulebook; and
 - b. any criminal or material civil action, charge or proceedings or Insolvency Proceedings, or any investigations, inspection or enquiries which may lead to any such action, charge or proceedings, made against the VASP or any of its Board members, UBOs or Senior Management immediately after the commencement of any such action, charge, proceeding, investigation, inspection or enquiry.
2. VASPs shall submit a report to VARA immediately upon the discovery of any violation or breach of any law, Regulation, Rule or Directive related to the conduct of any VA Activity.
3. VASPs shall, upon request from VARA, disclose information regarding their activities in jurisdictions other than the Emirate.
4. VASPs shall comply with all requirements in the Technology and Information Rulebook with regards to notifying VARA of incidents relating to a cybersecurity breach, including but not limited to incidents involving a loss of information or affecting Personal Data.

J. Staff Management and Training

1. VASPs shall implement procedures to ensure that they only employ suitably qualified individuals with the requisite skills, knowledge and expertise to perform the duties for which they are employed and that such individuals are duly registered with all applicable professional bodies as required.
2. VASPs shall employ appropriate numbers of Staff to discharge relevant duties effectively. Unless otherwise stated in the Regulations and Rulebooks, Staff are not required to be physically

located in the Emirate, provided that the VASP is able to ensure that all supervisory, monitoring and enforcement functions are effectively implemented to VARA's satisfaction.

3. VASPs shall ensure that all Staff are provided with adequate and up-to-date information regarding all their policies and procedures.
4. Adequate training suitable for the duties which the Staff is required to perform in their role shall be provided at the beginning of their employment and on an ongoing basis.
5. VASPs shall implement and provide AML/CFT training for all Staff on a regular basis and monitor their compliance with all established procedures.
6. VASPs shall make necessary arrangements to ensure that all operational policies and procedures are communicated to new hires within their first thirty (30) calendar days of starting their employment.
7. In the event that the operational policies and procedures are updated, VASPs shall ensure that—
 - a. relevant information is promptly communicated to all Staff; and
 - b. any such updated operational policies and procedures are made available to all Staff at all times.

Part II – Tax Reporting and Compliance

1. VASPs must, at all times, comply with all tax reporting obligations under all applicable laws, regulations, rules or guidance as well as national, international and industry best practices, including, but not limited to, under the United States Foreign Account Tax Compliance Act ("FATCA") where applicable.

Part III – Anti-Money Laundering and Combating the Financing of Terrorism

Introduction

Part III of this Compliance and Risk Management Rulebook sets out requirements which aim to prevent the use of Virtual Assets and services relating to them in furtherance of illicit activities. VARA considers such illicit activities to include money laundering and the financing of terrorism, as well as proliferation financing and sanctions non-compliance.

A. Appointment and Duties of Money Laundering Reporting Officer

1. VASPs shall appoint a Money Laundering Reporting Officer who—

- a. possesses at least two (2) years of experience handling AML/CFT matters; and
 - b. is a Fit and Proper Person ("MLRO").

Such appointment shall be reviewed annually to ensure that the MLRO remains a Fit and Proper Person capable of discharging all relevant duties. VARA has the sole discretion to request a VASP to provide such evidence as VARA may require which shows that the above requirements are satisfied. In addition, VARA shall take into consideration any failures by an individual to comply with Part III of this Compliance and Risk Management Rulebook when assessing whether an individual is a Fit and Proper Person.

2. The MLRO shall be responsible for—
 - a. ensuring the Board and Staff are properly and adequately trained in respect of their understanding and compliance with all applicable AML/CFT laws and regulatory requirements, particular those relevant to VA Activities;
 - b. developing and implementing AML/CFT policies and procedures as required under Rule III.B of this Compliance and Risk Management Rulebook;
 - c. conducting AML/CFT risk assessments in accordance with Rule III.D of this Compliance and Risk Management Rulebook and implementing all necessary changes to the VASP's relevant policies and procedures to address such issues and risks;
 - d. monitoring and reporting Suspicious Transactions in accordance with Rule III.F of this Compliance and Risk Management Rulebook;
 - e. if necessary, ensuring appropriate corrective actions are taken in response to non-compliance with any Federal AML-CFT Laws;
 - f. reporting to the Board on a quarterly basis on the effectiveness of the VASP's AML/CFT policies and procedures, identifying any failures in such policies and procedures and/or any non-compliance with any Federal AML-CFT Laws;
 - g. ensuring the quarterly reports required under Rule III.A.2.f of this Compliance and Risk Management Rulebook include a summary of all Anonymity-Enhanced Transactions and clients involved during that quarter; and
 - h. making the reports required under Rule III.A.2.f of this Compliance and Risk Management Rulebook available to VARA on request.
3. AML/CFT activities may be delegated to appropriate Entities, provided that—
 - a. the MLRO shall continue to be held accountable for all responsibilities and obligations in relation to the implementation of the relevant policies and procedures; and
 - b. all applicable requirements in the Company Rulebook, including Outsourcing management requirements, are complied with.
4. Subject to relevant requirements in the Company Rulebook and if deemed appropriate by the VASP, the MLRO may hold more than one (1) non-client facing role within the VASP, provided such roles do not create conflicting duties, including but not limited to, the CO and the head of the risk function. VARA will take into account other roles held by the MLRO in determining whether the individual is a Fit and Proper Person.

B. Policies and Procedures

1. VASPs will establish and implement policies and procedures to comply with all AML/CFT requirements and existing applicable laws, regulatory requirements and guidelines, including but not limited to—
 - a. the Federal AML-CFT Laws;
 - b. the Financial Action Task Force's (“**FATF**”) *12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (June 2020);
 - c. *FATF’s Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers* (July 2021);
 - d. *FATF’s Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (October 2021);

- e. the *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations* (March 2022);
- f. the UAE Executive Office for Control & Non-Proliferation (“EOCN”) *Guidance on Counter Proliferation Financing for FI’s, DNFBPs, and VASPs* (March 2022); and
- g. the EOCN’s Local Terrorist List, as may be amended from time to time.

2. To ensure compliance with the Federal AML-CFT Laws, such policies and procedures must establish courses of action allowing VASPs to—

- a. refrain from opening or conducting any financial or commercial transaction under an anonymous or fictitious name or by pseudonym or number, and maintaining a relationship or providing any services to it;
- b. ensure prompt application of the directives when issued by the competent authorities in the UAE for implementing United Nations Security Council Resolutions relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing, and other related directives, as well as compliance with all other applicable laws, regulatory requirements and guidelines in relation to economic sanctions;
- c. notwithstanding all relevant requirements in this Compliance and Risk Management Rulebook, maintain all records, documents, and data for all transactions, whether local or international, and make this information available to VARA upon request; and
- d. ensure full compliance with any other AML/CFT requirements and applicable laws, regulatory requirements and guidelines as may be promulgated by VARA, UAE federal government bodies, FATF or the Middle East and North Africa Financial Action Task Force from time to time.

3. VASPs shall establish adequate risk rules to screen clients, UBOs, Virtual Asset transactions and VA Wallet addresses to—

- a. identify potential illicit activities, potentially adverse information in higher risk situations (e.g. criminal history) and applicability of targeted or other international financial sanctions; and
- b. alert operation and compliance teams to impose relevant restriction and conduct further investigation.

4. All policies and procedures established and implemented pursuant to Rule III.B.1 of this Compliance and Risk Management Rulebook must be attested by a competent third party and shall be submitted to VARA in the licensing process and no more than twenty-one (21) calendar days after any changes coming into effect.

C. AML/CFT Controls

1. VASPs should have effective AML/CFT controls and systems in place which can adequately manage the AML/CFT risks relevant to their VA Activities, including the use of distributed ledger analytics tools, as well as other investigative tools or capabilities to monitor and screen transactions.
2. In respect of any distributed ledger analytics tools used, VASPs should review and document their review of the capabilities and weaknesses of such tools and design controls to monitor clients’ interaction with their VA Activities.
3. Information about Virtual Asset transactions and VA Wallet addresses are dynamic in nature. VASPs should review and document their review of the performance and function of any

distributed ledger analytics tools used to for ongoing monitoring.

4. VASPs shall, if applicable, implement internal controls to address the *FATF Report Virtual Assets Red Flags Indicators of Money Laundering and Terrorist Financing* (September 2020) (and any subsequent versions of, or supplements to, this publication) when designing transaction monitoring scenarios and thresholds to monitor clients' interaction with their VA Activities.

D. Risk Assessments

1. **Business risk assessment.** In implementing adequate and appropriate AML/CFT policies, procedures, and controls to detect and prevent illicit activities, VASPs must conduct AML/CFT business risk assessments.
2. The AML/CFT business risk assessments must be designed and implemented in order for VASPs to understand, identify and assess money laundering risks specific to their business and operations, taking into consideration their nature, size, and complexity. This includes, but is not limited to, identifying and assessing the AML/CFT risks in relation to the development and use of new or existing—
 - a. Virtual Assets (in particular, Anonymity-Enhanced Cryptocurrencies);
 - b. Virtual Asset related technologies, products or services (in particular, methods in which Anonymity-Enhanced Transactions can be conducted);
 - c. Virtual Asset related business and professional practices;
 - d. other technologies not specific to Virtual Assets (e.g. artificial intelligence and machine learning); and
 - e. other emerging risks.
3. Business risks assessments required under this Rule III.D must be carried out—
 - a. at regular intervals no longer than every three (3) months; and
 - b. in the event of a significant change or advancement in any of the areas listed in Rule III.D.2.
4. VASPs shall ensure, and be able to demonstrate to VARA on request, that the outcomes of business risk assessments directly inform—
 - a. the development and update of the VASP's AML/CFT policies, procedures, systems, and controls, including specific risk mitigation measures where appropriate; and
 - b. the areas in which the VASP prioritises the allocation of resources in its AML/CFT activities.
5. VASPs enabling Anonymity-Enhanced Transactions as part of their VA Activities must implement proportionately enhanced controls to ensure compliance with all applicable laws and regulations (including all Federal AML-CFT Laws), Regulations, Rules and Directives, as well as effectively monitor and prevent illicit uses. Such controls shall include conducting enhanced CDD on each client using those services, which shall be verified every six (6) months. In the case where the AML/CFT risks cannot be adequately mitigated, such products or services should not be offered.
6. **Client risk assessment.** In implementing adequate and appropriate AML/CFT policies, procedures, and controls to detect and prevent illicit activities, VASPs must conduct AML/CFT client risk assessments.
7. The AML/CFT client risk assessments must be designed and implemented in order for VASPs to understand, identify and assess money laundering risks specific to their client base and must

include, but not be limited to, identifying and assessing—

- a. the criteria and methodology for the categorisations of each client's AML/CFT risk;
- b. how such assessments are planned to be documented and associated courses of action to prevent illicit activity in each case based on the tiers of risk and probability of occurrence; and
- c. requirements for maintaining comprehensive audit trails of all risk assessments.

8. Client risk assessments required under this Rule III.D must be carried out at regular intervals no longer than every three (3) months.

E. Client Due Diligence

1. VASPs shall adopt a risk-based application of CDD measures in accordance with the Federal AML-CFT Laws.
2. VASPs shall undertake a risk-based assessment of every client using the criteria and methodology prescribed in the client risk assessment, required under Rules III.D.6 and III.D.7 above, and assign the client a risk rating proportionate to the assessed AML/CFT risks associated with that client.
3. VASPs are required to undertake CDD measures to verify the identity of the client and the UBO(s) before or during the establishment of a business relationship for the purposes of providing services relating to VA Activities, or before executing a transaction (whether or not denominated in Virtual Assets) for a client with whom there is no business relationship.
4. VASPs shall undertake CDD measures in the following circumstances—
 - a. when establishing a business relationship with a client for the purposes of providing services relating to VA Activities;
 - b. when carrying out occasional transactions in favour of a client for amounts equal to or exceeding AED 3,500, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
 - c. where there is an instruction from a client to handle a potential Suspicious Transaction;
 - d. where there are doubts about the veracity or adequacy of previously obtained identification information of a client; or
 - e. when carrying out any transaction for high-risk clients as characterised in the Federal AML-CFT Laws.
5. VASPs should undertake CDD measures in their ongoing supervision of business relationships with clients, including—
 - a. auditing transactions that are carried out throughout the period of the business relationship, to ensure that the transactions conducted are consistent with the information on file regarding clients and the risks they pose, including, where necessary, the source of funds; and
 - b. ensuring that the documents, data or information obtained from CDD measures are up-to-date and appropriate by regularly reviewing such records, particularly those of high-risk clients as characterised in the Federal AML-CFT Laws.
6. As part of the CDD process, VASPs shall verify clients' identity by reference to the following documents, data or information from a reliable and independent source—

- a. *For individuals—*
 - i. full name as shown on an identification card or a travel document (along with a copy of the original and valid identification card or travel document);
 - ii. nationality;
 - iii. address;
 - iv. place of birth;
 - v. name and address of employer; and
 - vi. if the client is a Politically Exposed Person, approval from the MLRO and a member of the Senior Management is required prior to establishing a business relationship with such client.
- b. *For Entities which are not individuals—*
 - i. full name of the Entity;
 - ii. type of Entity;
 - iii. constitutional documents (e.g. memorandum of association and articles of association) attested by competent authorities within the UAE;
 - iv. principle place of business;
 - v. names of individuals holding Senior Management positions in the Entity; and
 - vi. if the UBO is a Politically Exposed Person, approval from the MLRO and a member of the Senior Management is required prior to establishing a business relationship with such client.

7. VASPs are further required to—
 - a. verify that any Entity purporting to act on behalf of the client is so authorised, and verify the identity of that Entity in accordance with Rule III.E.6 of this Compliance and Risk Management Rulebook;
 - b. understand the intended purpose and nature of the business relationship with the client, and obtain, when necessary, information related to this purpose; and
 - c. where the VASP's client is a business or otherwise provides services to other clientele, understand the nature of the client's business as well as the client's ownership and control structure, including but not limited to the following—
 - i. the identity of UBO(s);
 - ii. whether such structure includes any DAOs and, if so, the intended purpose of such DAOs; and
 - iii. the type, nature and pursuits of the clientele of a prospective client and where necessary carry out appropriate due diligence on the client's clientele in order to ensure compliance with the Federal AML-CFT Laws.
8. If a VASP is unable to conduct appropriate CDD on a client, it shall not—
 - a. establish or maintain a business relationship with such client; or
 - b. execute any transaction for such client.

9. If a VASP relies on third parties to perform CDD, it shall remain liable for ensuring such third parties perform CDD in accordance with all relevant Rules and Directives. VASPs that rely on third parties to undertake CDD on their behalf must therefore implement adequate measures in keeping with the nature and size of their businesses (including VA Activities) to ensure that such third parties' performance of CDD is in accordance with all relevant Rules and Directives.
10. Enhanced CDD. If a VASP has assigned a client a high-risk rating in accordance with the client risk assessment required under Rules III.D.6 and III.D.7 above, or the client's UBO is a PEP, then in addition to all other CDD required in this Rule III.E, the VASP must—
 - a. obtain—
 - i. additional identification information for the client and all UBOs;
 - ii. additional information on the intended nature of the business relationship; and
 - iii. information on the reasons for a transaction;
 - b. update the CDD information which it holds on the client and any UBO more regularly;
 - c. identify and verify—
 - i. the source of funds; and
 - ii. the source of wealth of the client and, if applicable, all UBOs;
 - d. carry out enhanced monitoring of the business relationship, by increasing the frequency and intensity of controls applied, and determining which groups of transactions need further examination;
 - e. obtain the approval of Senior Management to commence a business relationship with the client;
 - f. require the first transaction into the client's account with the VASP to be carried out through an account in the customer's name with a licensed institution that is subject to AML/CFT laws and/or regulation and supervision in a jurisdiction that has standards equivalent to those set out in the FATF Recommendations; and
 - g. for a client who is a natural person, verify the current residential address (other than a post office box).

F. Suspicious Transaction Monitoring and Reporting

1. VASPs shall employ methods which are appropriate to their particular circumstances and VA Activities, to continuously monitor business relationships with clients to identify any Suspicious Transactions and where an AML-CFT Report is required to be made. Such methods shall ensure that no 'tipping-off' or similar offence occurs. Such methods shall also ensure all Suspicious Transactions are immediately reported to the MLRO, in order for the MLRO to meet the requirements of this Rule III.F. VASPs are required to document, obtain Senior Management approval for, and periodically review and update such methods to ensure their effectiveness.
2. VASPs shall put in place and regularly update indicators that can be used to identify possible Suspicious Transactions and where an AML-CFT Report is required to be made.
3. Upon suspicion or reasonable grounds to suspect that the proceeds of a transaction are related to a crime, or the attempt or intention to use funds or proceeds for the purpose of committing, concealing or benefitting from a crime, the MLRO shall be responsible for—

- a. immediately reporting to the UAE FIU such Suspicious Transactions in accordance with Rule III.F.4 of this Compliance and Risk Management Rulebook;
- b. responding to all additional information requests from the UAE FIU and/or VARA promptly and in any event within forty-eight (48) hours of such requests;
- c. undertaking any additional actions as may be requested by the UAE FIU and/or VARA within any specified timeframe in such requests; and
- d. in the event the MLRO is not the same individual as the CO, immediately reporting to the CO that a Suspicion Transaction report has been made, provided that the provision of any such report would not be considered 'tipping-off' or a similar offence under any applicable laws or regulations.

4. AML-CFT Reports shall be made—
 - a. to the UAE FIU on the GoAML platform or by any other means approved by the UAE FIU;
 - b. in the form and containing all content required by the UAE FIU and VARA from time to time; and
 - c. in accordance with any Guidance which may be issued by VARA from time to time.
5. VASPs shall continue monitoring (on a near real time basis where appropriate) any transactions which are the subject of an AML-CFT Report.

G. FATF Travel Rule

1. VASPs must comply with all Federal AML-CFT Laws, including but not limited to Travel Rule requirements as prescribed in Federal AML-CFT Laws. In addition to all requirements in Federal AML-CFT Laws, VASPs must comply with this Rule III.G as a minimum standard that may be supplemented by additional requirements in Federal AML-CFT Laws.
2. Prior to initiating any transfer of Virtual Assets with an equivalent value exceeding AED 3,500, VASPs must obtain and hold required and accurate originator information and required beneficiary information, and make it available on request to VARA and/or other appropriate authorities. The specific requirements for obtaining, holding and transmitting this information shall be as prescribed in Federal AML-CFT Laws and as may be incrementally defined by VARA from time to time.
3. Prior to permitting any clients access to Virtual Assets received from a transfer with an equivalent value exceeding AED 3,500, a beneficiary VASP must obtain and hold required originator information and required and accurate beneficiary information, and make it available on request to VARA and/or other appropriate authorities. The specific requirements for obtaining, holding and transmitting this information shall be as prescribed in Federal AML-CFT Laws and as may be incrementally defined by VARA from time to time.
4. Subject to additional requirements prescribed in Federal AML-CFT Laws, the minimum required originator information shall include, but not be limited to, the originator's—
 - a. name;
 - b. account number or VA Wallet address; and
 - c. residential or business address.
5. Subject to additional requirements prescribed in Federal AML-CFT Laws, the minimum required beneficiary information shall include, but not be limited to, the beneficiary's—

- a. name; and
- b. account number or VA Wallet address.

6. Prior to entering into any transaction with a counterparty VASP or virtual asset service provider in any other jurisdiction, VASPs must complete risk-based due diligence on such counterparty in order to mitigate AML/CFT risks. This due diligence does not need to be completed for every subsequent transaction with the counterparty unless a heightened counterparty risk is assessed or identified.

7. In complying with the Travel Rule, VASPs must consider how they will handle the risks associated with—

- a. deposits or withdrawals (including those which are compliant with the Travel Rule and those which are not);
- b. non-obliged entities (i.e. unhosted VA Wallets); and
- c. Anonymity-Enhanced Transactions.

8. VASPs shall be required to demonstrate to VARA how they comply with the Travel Rule during the licensing process and submit to VARA relevant policies and controls. VASPs should also include their plan to comply with the Travel Rule with virtual asset service providers in jurisdictions where the Travel Rule is not a legislative requirement (i.e. the ‘sunrise issue’).

9. In implementing policies and controls to comply with the Travel Rule and AML/CFT Rules, VASPs shall be guided by *FATF Interpretive Note to Recommendation 15* and all applicable regulatory requirements and guidelines as may be in force from time to time. VASPs must monitor for any transaction or series of transactions that seeks to circumvent any regulatory thresholds to bypass Travel Rule requirements.

10. VARA may require VASPs to report on their compliance with the Travel Rule and the effectiveness of their implementing policies and controls, at any time. VASPs must report on Travel Rule compliance in accordance with all requirements in Federal AML-CFT Laws and any additional requirements as may be specified by VARA.

H. Compliance with targeted financial sanctions

1. Screening. VASPs must screen all clients and transactions against lists of designated Entities maintained under—
 - a. the UNSC sanctions frameworks; and
 - b. Federal AML-CFT Laws.
2. VASP are required to—
 - a. implement automated screening systems to identify and flag transactions involving designated Entities from the UNSC sanctions frameworks or Federal AML-CFT Laws; and
 - b. ensure that such systems are updated regularly with the latest sanctions lists and operate in real-time.
3. Freezing. VASPs are required to—
 - a. take immediate action to freeze any assets, including Virtual Assets and/or money, associated with individuals or entities identified as designated Entities under the UNSC

- sanctions frameworks or Federal AML-CFT Laws; and
- b. ensure that no withdrawals, transfers, or use of the frozen assets occur during the freezing period.

4. VASPs must establish and enforce internal policies and procedures to—

- a. immediately freeze any assets, including Virtual Assets and/or money, upon detecting a match with a designated Entity; and
- b. maintain records of all freezing actions and associated transactions for a minimum of eight (8) years.

5. Prohibition of transactions. VASPs must block and prohibit—

- a. any transactions involving individuals, organisations, or entities listed under the UNSC sanctions frameworks or Federal AML-CFT Laws; and
- b. any attempts by clients to bypass the UNSC sanctions frameworks or Federal AML-CFT Laws.

I. Record keeping

1. VASPs shall retain the following types of records relating to AML/CFT in accordance with Federal AML-CFT Laws—
 - a. Virtual Asset transaction records, including operational and statistical records, documents and information (whether or not recorded on public distributed ledgers) concerning all transactions executed or processed by the VASP;
 - b. CDD records, including records, documents, and information about clients (e.g. account files and business correspondence), and results from the investigation and analysis of clients' activities;
 - c. information relating to third parties engaged by the VASP to undertake CDD;
 - d. records relating to ongoing monitoring of business relationships with clients; and
 - e. Suspicious Transaction reports made in accordance with Rule III.F of this Compliance and Risk Management Rulebook.
2. VASPs shall retain all records required in Rule III.I.1 for a period of no less than eight (8) years.

J. Enforcement

1. VASPs which fail to comply with Rules in this Part III of the Compliance and Risk Management Rulebook may be subject to enforcement actions taken by VARA or other penalties as set out in the Regulations and Federal AML-CFT Laws.
2. Enforcement action(s) taken by VARA for a VASP's failure to comply with the Rules in this Part III of the Compliance and Risk Management Rulebook may be taken directly against the VASP, its directors, Responsible Individuals, MLRO and/or Senior Management.

Part IV – Client Money Rules

A. Application and Interpretation

1. **“Client Money”** means all money owned by a VASP’s client which is held or controlled by a VASP on behalf of such client in the course of, or in connection with, the carrying on of any VA Activity, except for—
 - a. money which is immediately due and payable to a VASP for the VASP’s own account, such as fees for services provided to a client;
 - b. amounts payable by the VASP for expenses incurred on behalf of the client; and
 - c. other charges that are due and payable to the VASP.
2. Client Money does not include any Virtual Assets held by a VASP on behalf of a client.
3. Client Money is held or controlled by a VASP if it is—
 - a. directly held by the VASP;
 - b. held in an account in the name of the VASP; or
 - c. held by an Entity, or in an account in the name of an Entity, controlled by the VASP.
4. **“Client Account”** means an account at a Third-Party Bank which—
 - a. holds or is established to hold the Client Money of one or more clients; and
 - b. is maintained in the name of the VASP.
5. **“Third-Party Bank”** means the bank with which a Client Account is maintained.

B. Treatment of Client Money

1. VASPs must have in place the necessary policies, systems and controls, appropriate to the nature and scale of their operations, to ensure compliance with this Part IV of the Compliance and Risk Management Rulebook.
2. VASPs holding Client Money must hold it for their clients in a Client Account. Client Money is not owned by the VASP and shall not form part of the VASP’s estate in the event that the VASP is or becomes Insolvent.
3. All Client Accounts must include the words “Client Account” in their title.
4. VASPs must have systems and controls to ensure that the Client Money is identifiable and secure at all times.
5. Where a VASP holds or controls Client Money it must ensure—
 - a. except where otherwise provided in Rule IV.B.6 of this Compliance and Risk Management Rulebook, that the Client Money is paid into a Client Account within one (1) calendar day of receipt;
 - b. Client Money held or controlled on behalf of clients in the UAE is paid into Client Accounts maintained with Third-Party Banks in the UAE; and
 - c. Client Money held or controlled on behalf of clients outside of the UAE may be deposited into Client Accounts with Third-Party Banks outside of the UAE but must be moved to, and maintained with, Third-Party Banks in the UAE, and VASPs must initiate such moves within twenty-four (24) hours of receipt.

6. The requirement for a VASP to pay Client Money into a Client Account does not, subject to Rule IV.B.7 of this Compliance and Risk Management Rulebook, apply with respect to such Client Money—
 - a. temporarily held by the VASP before forwarding to an Entity nominated by the client;
 - b. in connection with a delivery versus payment transaction where—
 - i. in respect of a client purchase, Client Money from the client will be due to the VASP within one (1) calendar day upon the fulfilment of a delivery obligation; or
 - ii. in respect of a client sale, Client Money will be due to the client within one (1) calendar day following the client's fulfilment of a delivery obligation; or
 - iii. held in the client's own name where the VASP has a mandate to manage the Client Money on a discretionary basis.
7. VASPs must pay Client Money of the type described in Rule IV.B.6.b of this Compliance and Risk Management Rulebook into a Client Account where they have not fulfilled their delivery or payment obligation within three (3) calendar days of receipt of the Client Money.
8. VASPs must maintain adequate records of all payments of Client Money received including, in respect of each payment, the—
 - a. date of receipt;
 - b. name and unique identifier of the client for whom payment is to be credited;
 - c. name of the Entity who made the payment;
 - d. transaction identifier and/or reference; and
 - e. date when the payment was presented to the VASP's Third-Party Bank.
9. Payment into Client Accounts.
 - a. VASPs must maintain systems and controls for identifying money which must not be in a Client Account and for transferring it without delay.
 - b. VASPs must not hold or deposit their own money into a Client Account, except where—
 - i. it is a minimum sum required to open the account, or to keep it open;
 - ii. the money is received by way of mixed remittance, provided the VASP transfers out that part of the payment which is not Client Money within one (1) calendar day of the day on which the VASP would normally expect the remittance to be cleared;
 - iii. interest credited to the account exceeds the amount payable to clients, as applicable, provided that the money is removed within twenty (20) calendar days; or
 - iv. it is to meet a temporary shortfall in Client Money.
10. Payment out of Client Accounts.
 - a. VASPs must have procedures for ensuring all withdrawals from a Client Account are authorised.
 - b. Client Money must remain in a Client Account until it is—
 - i. due and payable to the VASP;
 - ii. paid to the client on whose behalf the Client Money is held;
 - iii. paid in accordance with a client's instruction on whose behalf the Client Money is held;

- iv. required to meet the payment obligations of the client on whose behalf the Client Money is held; or
- v. paid out in circumstances that are otherwise authorised by VARA.

- c. VASPs must not use Client Money belonging to one client to satisfy an obligation owed to another client, nor for any other obligation owed to other Entities (including but not limited to for liquidity, capital ratios or their own balance sheet purposes).
- d. VASPs must have a system for ensuring no off-setting or debit balances occur in Client Accounts.

11. In addition to all requirements in Rule II.B of the Market Conduct Rulebook, VASPs shall not take ownership of Client Money under any Client Agreement.

12. By way of limited exception to Rule IV.B.11 of this Compliance and Risk Management Rulebook, VASPs are permitted to take ownership of Client Money for the limited purpose of placing such money under trust, where the VASP is the founder and the VASP's client(s) are the beneficiaries of that trust, and provided that—

- a. the ownership of all Client Money must be transferred to the trust in accordance with all other provisions of this Part IV Client Money Rules of the Compliance and Risk Management Rulebook; and
- b. the VASP must continue to comply with all other provisions of this Part IV Client Money Rules of the Compliance and Risk Management Rulebook, at all times.

C. Third-Party Bank

- 1. VASPs may only maintain Client Accounts at Third-Party Banks appropriately and validly authorised to accept or take deposits in accordance with applicable laws and regulatory requirements in the relevant jurisdiction and which must not be in the same Group as the VASP.
- 2. Payment of Client Money to a Third-Party Bank.
 - a. VASPs may only pass, or permit to be passed, Client Money to a Third-Party Bank if—
 - i. the Client Money is to be used in respect of a transaction or series of transactions for that client; and
 - ii. the Third-Party Bank is appropriately and validly authorised to accept or take deposits in accordance with applicable laws and regulatory requirements in its relevant jurisdiction as per Rule IV.C.1 of this Compliance and Risk Management Rulebook.
- 3. When a VASP opens a Client Account with a Third-Party Bank, it must promptly obtain a written acknowledgement from the Third-Party Bank stating that—
 - a. all money standing to the credit of the account is held by the VASP as agent and that the Third-Party Bank is not entitled to combine the account with any other account or to exercise any charge, mortgage, lien, right of set-off or counterclaim against money in that account in respect of any sum owed to it on any other account of the VASP; and
 - b. the title of the account sufficiently distinguishes that account from any account containing money that belongs to the VASP, and is in the form requested by the VASP.

4. If the Third-Party Bank does not promptly provide the acknowledgement referred to in Rule IV.C.3 of this Compliance and Risk Management Rulebook, the VASP must refrain from making further deposits of Client Money with that Third-Party Bank and withdraw any Client Money in that Client Account.

D. Disclosure, Reporting and Audit Requirements

1. Proper record keeping.
 - a. VASPs shall keep proper and up-to-date records regarding—
 - i. the receipt and payment of Client Money and in and out of Client Accounts; and
 - ii. movements of Client Money within internal systems,to enable the reconciliation of any differences in balances or positions of Client Money.
 - b. VASPs shall have appropriate procedures for identifying Client Money received. The procedures should cover Client Money received through all means, including electronically or via agents of the VASP (e.g. banks, payment processors).
 - c. VASPs may be requested to demonstrate evidence of above records upon VARA's request.
2. Client reporting.
 - a. VASPs must send or otherwise make available a statement to clients at least monthly, or as agreed with the client, which shall include—
 - i. the client's total Client Money balances held by the VASP;
 - ii. the amount, date and value of each credit and debit paid into and out of the account since the previous statement; and
 - iii. any interest earned or charged on the Client Account since the previous statement.
 - b. The statement sent to the client must be prepared within twenty-five (25) calendar days of the statement date.

E. Reconciliation

1. VASPs must maintain a system to ensure that accurate reconciliations of the Client Accounts are carried out daily. The reconciliation must include—
 - a. a full list of individual client credit ledger balances, as recorded by the VASP;
 - b. a full list of individual client debit ledger balances, as recorded by the VASP;
 - c. a full list of outstanding lodgements;
 - d. a full list of Client Account cash book balances; and
 - e. formal statements from Third-Party Banks showing account balances as at the date of reconciliation.
2. VASPs must—

- a. reconcile the individual credit ledger balances, Client Account cash book balances and the Third-Party Bank Client Account balances;
- b. check that the balance in the Client Accounts as at the close of business on the previous day was at least equal to the aggregate balance of individual credit ledger balances as at the close of business on the previous day; and
- c. ensure that all shortfalls, excess balances and unresolved differences, other than differences arising solely as a result of timing differences between the accounting systems of the Third-Party Bank and the VASP, are investigated and, where applicable, corrective action taken as soon as possible, including where necessary using the VASP's own funds.

3. VASPs must perform the reconciliations in Rule IV.E.2 of this Compliance and Risk Management Rulebook on a daily basis.
4. VASPs must ensure that the process of reconciliation does not give rise to a conflict of interest.
5. VASPs must notify VARA where there has been a material discrepancy with the reconciliation which has not been rectified.

F. Failure to Comply

1. VASPs which become aware that they do not comply with any Rules in this Part IV of the Compliance and Risk Management Rulebook must notify VARA in writing of any such non-compliance within one (1) calendar day.
2. Failure to comply with any Rules in this Part IV of the Compliance and Risk Management Rulebook may result in VARA taking appropriate enforcement action(s) as it deems fit and the VASP must comply with all corrective action(s) as instructed by VARA.

Part V – Client Virtual Assets Rules

A. Application and Interpretation

1. “**Client VAs**” means all Virtual Assets owned by a VASP’s client which are held or controlled by a VASP on behalf of such client in the course of, or in connection with, the carrying on of any VA Activity, except for—
 - a. Virtual Assets immediately due and payable to a VASP for the VASP’s own account, such as fees for services provided to a client;
 - b. amounts payable by the VASP for expenses incurred on behalf of the client; and
 - c. other charges that are due and payable to the VASP.
2. Client VAs are held or controlled by a VASP if they are—
 - a. directly held by the VASP in an account or VA Wallet;
 - b. held in an account or VA Wallet in the name of the VASP;
 - c. held by a legal entity, or in an account or VA Wallet in the name of a legal entity, controlled by the VASP; or
 - d. the private keys and/or seed phrase of the VA Wallet are held or controlled by the VASP.

B. Treatment of Client VAs

1. VASPs must have in place the necessary policies, systems and controls, appropriate to the nature and scale of their operations, to ensure compliance with this Part V of the Compliance and Risk Management Rulebook.
2. Client VAs are not depository liabilities or assets of the VASP. Client VAs are not owned by the VASP and shall not form part of the VASP's estate in the event that the VASP is or becomes Insolvent.
3. VASPs shall hold Client VAs in separate VA Wallets from all Virtual Assets of the VASP. VASPs must include the label 'Client VA Wallet' in their books and records for all wallets holding Client VAs at all times.
4. VASPs must hold Client VAs on a one-to-one basis and shall not authorise or permit rehypothecation of Client VAs, unless they have explicit prior consent from the client providing discretionary authority to do so, and are appropriately authorised and Licensed by VARA to carry out all relevant VA Activity(ies) in respect of such Virtual Assets.
5. All proceeds related to Client VAs, such as 'airdrops', 'staking gains' or similar proceeds shall accrue to the client's benefit, unless the VASP has the client's prior consent specified in a written agreement with the client or otherwise. VASPs may decide not to collect or distribute certain proceeds, including where such proceeds are below a value to be determined by the VASP, provided that the VASP has disclosed this to the client and obtained acceptance in accordance with all applicable laws.
6. In addition to all requirements in Rule II.B of the Market Conduct Rulebook, VASPs shall not take ownership of Client VAs under any Client Agreement.
7. By way of limited exception to Rule V.B.6 of this Compliance and Risk Management Rulebook, VASPs are permitted to take ownership of Client VAs for the limited purpose of placing such Virtual Assets under trust, where the VASP is the founder and the VASP's client(s) are the beneficiaries of that trust, and provided that—
 - a. the ownership of all Client VAs must be transferred to the trust no more than one (1) calendar day from receipt of the Virtual Assets by the VASP; and
 - b. the VASP must continue to comply with all other provisions of this Part V Client Virtual Asset Rules of the Compliance and Risk Management Rulebook, at all times.

C. Proof of Reserves

1. In addition to the Reserve Assets requirements in the Company Rulebook, VASPs shall comply with all requirements stipulated by VARA from time to time, including as part of a VASP's licensing process, in order to demonstrate that assets held in reserve cover all of their liabilities with respect to Client VAs.

D. Reconciliation

1. VASPs must maintain a system to ensure that accurate reconciliations of the Virtual Assets owned by each client are carried out daily. The reconciliation must include—
 - a. a full list of individual client credit ledger balances, as recorded by the VASP; and
 - b. a full list of individual client debit ledger balances, as recorded by the VASP.
2. VASPs must notify VARA where there has been a material discrepancy with the reconciliation which has not been rectified.

Part VI – Anti-Bribery and Corruption

A. General Principles

1. VASPs shall establish and maintain an effective anti-bribery and corruption policy to ensure that the Board and all Staff must comply with all applicable laws and regulations relevant to anti-bribery and corruption in all jurisdictions in which they operate. Such policy must allow for reports to be made by Entities outside of the VASP and protect the identity and confidentiality of the Entity who has made a report at all times.
2. VASPs must conduct all business in an honest and ethical manner and must take a zero-tolerance approach to bribery and corruption. The Board and all Staff must act professionally, fairly and with integrity in all business dealings and relationships.
3. It is prohibited for any VASP, members of the Board and all Staff, to—
 - a. give, promise to give, or offer a payment, gift or hospitality to a third party or otherwise engage in or permit a bribery offence to occur, with the expectation or hope that an advantage in business will be received or to reward a business advantage already given;
 - b. give, promise to give, or offer a payment, gift or hospitality to a third party to facilitate or expedite a routine procedure;
 - c. accept a payment, gift or hospitality from a third party if it knows or suspects that such payment, gift or hospitality is offered or provided with an expectation that a business advantage will be provided by the VASP in return;
 - d. threaten or retaliate against another member of the Board or Staff who has refused to commit a bribery offence or who has raised concerns; and
 - e. engage in any activity that might lead to a breach of the anti-bribery and corruption Rules in this Part VI of the Compliance and Risk Management Rulebook.
4. The anti-bribery and corruption Rules in this Part VI of the Compliance and Risk Management Rulebook do not prohibit normal and appropriate hospitality (given or received in accordance with the VASP's own gifts and hospitality policy) to or from third parties, provided relevant policies are compliant with applicable laws. Such gifts and hospitality policy should set out clearly what is and is not appropriate to make or receive gifts and/or hospitality to and from a third party.
5. The CO will monitor the effectiveness of the anti-bribery and corruption policy on a regular basis. Any deficiencies identified should be dealt with as soon as possible.

B. No Corrupt Payments

1. It is prohibited for any VASP or any members of its Board, Staff, consultants or contractors, any Group company, agent, business partner, contractor or supplier of the VASP to make any payment(s) to a third party where there is any reason to believe that all or any part of such payment will go towards a bribe or otherwise facilitate any corruption.
2. All payments made by VASPs for services must be appropriate and justifiable for the purpose of legitimate services provided.

C. Investigation and Reporting

1. VASPs must establish, maintain and publish methods of contact including, but not limited to, a telephone line, for receiving reports of any violation or possible violation of any applicable laws

and regulations relevant to anti-bribery and corruption by the VASP, or its Board or Staff on its behalf.

2. Any member of the Board or Staff must report to the CO as soon as possible if they believe or suspect that an action in conflict with the anti-bribery and corruption Rules in this Part VI of the Compliance and Risk Management Rulebook has occurred, or may occur, or has been solicited by any other Entity.
3. The CO shall investigate any report of a violation or possible violation of the anti-bribery and corruption Rules in this Part VI of the Compliance and Risk Management Rulebook and shall follow the below procedures—
 - a. An investigation file should be opened. In the case of an oral report, the CO should prepare a written summary.
 - b. The CO shall appoint an independent Entity who shall promptly commission the conduct of an investigation. The investigation will document all relevant facts, including Entities involved, times and dates.
 - c. The CO shall advise the Board of the existence of an investigation.
 - d. The identity of the individual disclosing relevant information to the CO should be treated in accordance with applicable UAE laws and regulations.
 - e. On completion of the investigation, a written investigation report will be provided by the Entity employed to conduct the investigation to the CO. If any unlawful conduct is found, the CO must advise the Board accordingly.
 - f. If any unlawful conduct is found, the VASP shall take such remedial action as the Board deems appropriate to achieve compliance with its internal anti-bribery and corruption policy and all applicable anti-bribery and corruption laws. The Entity employed to conduct the investigation shall prepare a written summary of the remedial actions taken.
 - g. The written investigation report and a written summary of the remedial actions taken shall be retained by the CO for a period of no less than eight (8) years from completion of the remedial action. Such reports shall be made available to VARA upon request.

D. Information and Trainings

1. VASPs shall implement and provide an anti-bribery and corruption training programme for the Board and all Staff on a regular basis and monitor their compliance with all established procedures. All members of the Board and Staff must participate in all such trainings provided by the VASP.
2. VASPs shall ensure that all members of the Board and Staff to have full access at all times to the most up-to-date anti-bribery and corruption policy and will be informed of any changes to such policy.
3. Training on the anti-bribery and corruption policy should form part of the induction programme made available to all new Board members and Staff.
4. In addition to relevant requirements in the Market Conduct Rulebook, a zero-tolerance approach to bribery and corruption and all relevant policies must be disclosed by all VASPs to the public and communicated at the outset of all business relationships as appropriate.

E. Responsibility for the Policy

1. The Board shall have the overall responsibility for ensuring its anti-bribery and corruption policy is up-to-date and complies with all applicable laws and regulations in all jurisdictions where the VASP conducts its business.

2. The CO has the primary and day-to-day responsibility for implementing the anti-bribery and corruption policy and for monitoring its effectiveness.

F. Consequences of Breach

1. Failure to comply with a VASP's anti-bribery and corruption policy should result in severe consequences, including internal disciplinary action and termination of employment without notice.
2. VASPs should immediately report to VARA any finding of unlawful conduct in breach of the anti-bribery and corruption Rules in this Part VI of the Compliance and Risk Management Rulebook.

Part VII – Sponsored VASPs

A. Interpretation

1. "**Regulated Sponsor**" means a VASP which is approved by VARA to sponsor other Entities to carry out one or more VA Activities in the Emirate, in accordance with this Part VII of the Compliance and Risk Management Rulebook.
2. "**Sponsored VASP**" means an Entity which is sponsored by a Regulated Sponsor to carry out one or more VA Activities in the Emirate, in accordance with this Part VII of the Compliance and Risk Management Rulebook.

B. Requirement to Obtain Prior Approval

1. No VASP may act as a Regulated Sponsor without approval from VARA in accordance with Rule VII.C of this Part VII of the Compliance and Risk Management Rulebook, below.
2. For the avoidance of doubt, nothing in this Part VII of the Compliance and Risk Management Rulebook shall have any effect on a VASP's obligations to comply with all other requirements in the Regulations, Marketing Regulations, Rulebooks, Directives and/or their Licence in respect of the VA Activities for which it is otherwise Licensed to carry out.

C. Application Process

1. VASPs shall adhere to the application process as prescribed by VARA from time to time, when applying for approval to be a Regulated Sponsor pursuant to this Part VII of the Compliance and Risk Management Rulebook.
2. All applications for approval shall, at a minimum, consist of the following—
 - a. demonstration of the Regulated Sponsor's ability to comply with this Part VII of the Compliance and Risk Management Rulebook; and
 - b. demonstration of the Regulated Sponsor's ability to ensure all Sponsored VASPs comply with all Regulations, Marketing Regulations, Rules and Directives applicable to the VA Activities which the Sponsored VASPs will carry out, and on an ongoing basis, as may be amended from time to time.

D. Establishing a Sponsored VASP Relationship

1. In order to establish a Sponsored VASP relationship, a Regulated Sponsor must—
 - a. be the Controlling Entity of, or have the same Controlling Entity as, the Sponsored VASP;
 - b. have a written agreement with each Sponsored VASP, which shall include—
 - i. what business and/or VA Activities the Sponsored VASP can carry out;
 - ii. apportioning liability for compliance in areas not prescribed by VARA;
 - iii. state clearly when and how the agreement can be terminated;
 - iv. provide the Regulated Sponsor with rights of audit over the Sponsored VASP; and
 - v. require the Sponsored VASP to report regularly to the Regulated Sponsor on the Sponsored VASP's compliance with its obligations under this Compliance and Risk Management Rulebook;
 - c. conduct detailed due diligence and assess each Sponsored VASP before sponsoring them, to ensure they're fit and proper, financially stable and suitable to carry out their proposed VA Activities;
 - d. ensure that establishing such relationship does not contravene Federal Competition Laws; and
 - e. obtain approval from VARA, through the process prescribed by VARA from time to time, prior to the Sponsored VASP commencing any VA Activities in the Emirate under the Sponsored VASP relationship.
2. Legal entity in the Emirate. Regulated Sponsors shall ensure that each Sponsored VASP is and remains a legal entity, in one of the legal forms approved by a commercial licensing authority, in the Emirate.
3. VARA reserves the right to refuse, suspend or revoke approval of any Sponsored VASP relationship on any grounds, including but not limited to, where VARA deems, in its sole and absolute discretion, that such relationship may create an anti-competitive or monopolistic position or otherwise threaten the integrity and/or stability of the Virtual Assets market in the Emirate.

E. Regulatory Status, Marketing and Disclosures

1. Regulatory status. Notwithstanding Rule VII.E.2.c of this Compliance and Risk Management Rulebook, for the purposes of Regulation III.A.1.a of the Regulations, all Sponsored VASPs established and maintained in accordance with this Part VII of the Compliance and Risk Management Rulebook, shall be deemed as authorised and Licensed by VARA for the VA Activities which the application for approval under Rule VII.D of this Compliance and Risk Management Rulebook relates and as approved by VARA under Rule VII.D.1.e.
2. Marketing. In all Marketing, Regulated Sponsors shall ensure that Sponsored VASPs—
 - a. comply with the Marketing Regulations;
 - b. include the name and Licence number of the Regulated Sponsor; and
 - c. clearly indicate that they are a Sponsored VASP, and not a VARA Licensed VASP.
3. Public disclosures and risk disclosure statement. In addition to all other requirements regarding disclosures required under the Regulations, Marketing Regulations, Rules or Directives, Regulated Sponsors shall ensure that all Sponsored VASPs provide the following information in an easily accessible location, in a machine-readable format, and that it is kept accurate and up-

to-date at all times—

- a. the name of their Regulated Sponsor and the Licence number issued to the Regulated Sponsor by VARA;
- b. the authorisation number issued to the Sponsored VASP by VARA;
- c. all VA Activities they are authorised by VARA to carry out in the Emirate, including any restrictions stated by VARA as a condition of their authorisation, and the validity period of such authorisation; and
- d. the name of the Sponsored VASP's Responsible Officer appointed in accordance with Rule VII.G below.

F. Compliance Responsibility

1. Regulated Sponsors shall ensure, and be responsible for, the ongoing compliance with all applicable Regulations, Marketing Regulations, Rules and Directives by their Sponsored VASPs, at all times.
2. Regulated Sponsors shall ensure that they have sufficient resource, knowledge and expertise to comply with their obligations in this Part VII of the Compliance and Risk Management Rulebook, at all times, in respect of each Sponsored VASP and all Sponsored VASP relationships in total.
3. Regulated Sponsors shall, at all times, ensure and be responsible for their Sponsored VASPs' compliance with the following compulsory Rulebooks as may be updated from time to time—
 - a. Company Rulebook;
 - b. Compliance and Risk Management Rulebook;
 - c. Technology and Information Rulebook; and
 - d. Market Conduct Rulebook.
4. Regulated Sponsors shall, at all times, ensure and be responsible for their Sponsored VASPs' compliance with all relevant Rulebooks that correspond to the VA Activities the Sponsored VASP is authorised by VARA to carry out, as may be amended from time to time—
 - a. Advisory Services Rulebook;
 - b. Broker-Dealer Services Rulebook;
 - c. Custody Services Rulebook;
 - d. Exchange Services Rulebook;
 - e. Lending and Borrowing Services Rulebook;
 - f. VA Management and Investment Services Rulebook; and
 - g. VA Transfer and Settlement Services Rulebook.
5. Data protection and segregation. In addition to all Rules in Part II of the Technology and Information Rulebook, Regulated Sponsors must ensure that Personal Data collected by each Sponsored VASP remains segregated from that of the Regulated Sponsor, and each of the Regulated Sponsor's other Sponsored VASPs.

G. Responsible Officer

1. Regulated Sponsors must ensure their Sponsored VASPs each appoint one (1) individual of sufficient seniority who shall be responsible for the Sponsored VASP's compliance with all legal

and regulatory obligations (“**Responsible Officer**”).

2. The Responsible Officer must be—
 - a. a full-time employee of the Sponsored VASP;
 - b. notified to, and approved by, VARA during the application process in Rule VII.D of this Compliance and Risk Management Rulebook; and
 - c. meet all other requirements in Rule I.C.2 of the Company Rulebook, as may be amended from time to time.
3. Regulated Sponsors must ensure that the Responsible Officer continues to meet the requirements in Rule VII.G.2 of this Compliance and Risk Management Rulebook at all times, and shall validate and maintain a record of such validation on an annual basis.
4. Regulated Sponsors must notify and seek approval from VARA prior to changing the Responsible Officer of any Sponsored VASP, except in the event of reasonably unforeseen circumstances. In such instances, the Regulated Sponsor must notify VARA immediately and provide information on how it will continue to meet the requirements with regard to the Responsible Officer of the Sponsored VASP.

H. Capital and Prudential Requirements

1. In addition to all existing obligations in respect of the VA Activities for which it is Licensed, Regulated Sponsors shall comply with Part VI Capital and Prudential Requirements of the Company Rulebook for each Sponsored VASP with whom it has a Sponsored VASP relationship.

I. Accounts

1. Subject to compliance with Rule VII.I.2 of this Compliance and Risk Management Rulebook below, Regulated Sponsors may establish each of the following accounts in their own name on behalf of each Sponsored VASP—
 - a. Client Money Accounts required in Part IV of this Compliance and Risk Management Rulebook;
 - b. business and/or operating accounts of the Sponsored VASP; and
 - c. an account maintaining Paid-Up Capital in accordance with Rule VI.B.3 of the Company Rulebook.
2. Regulated Sponsors must ensure, and are responsible for ensuring, that each of the accounts listed in Rule VII.I.1 of this Compliance and Risk Management Rulebook above comply with the following—
 - a. a separate account is established for each Sponsored VASP with whom it has a Sponsored VASP relationship, and no account is shared either between the Regulated Sponsor and a Sponsored VASP, or between more than one Sponsored VASP;
 - b. the name of the Sponsored VASP is included in the title of each account; and
 - c. the Regulated Sponsor maintains segregation between all the accounts of each Sponsored VASP, with whom it has a Sponsored VASP relationship, in all books and records.

J. Complaints Handling Requirements

1. Regulated Sponsors must ensure, and are responsible for ensuring, compliance with Part III of the Market Conduct Rulebook for each Sponsored VASP with whom it has a Sponsored VASP relationship.
2. Regulated Sponsors must establish, or ensure each Sponsored VASP establishes, a separate Complaints handling procedure required in Part III.B of the Market Conduct Rulebook for each Sponsored VASP with whom it has a Sponsored VASP relationship.

K. Governance and Reporting Responsibilities

1. Governance. Regulated Sponsors must—
 - a. review and maintain oversight of each Sponsored VASP's activities, business and senior management;
 - b. monitor and actively manage each Sponsored VASP's performance of its obligations under the written agreement between the Sponsored VASP and the Regulated Sponsor, as required under Rule VII.D.1.b of this Compliance and Risk Management Rulebook;
 - c. ensure that they have the skills and resources to oversee all Sponsored VASPs at all times, including if a Sponsored VASP's business changes and/or expands;
 - d. ensure that each Sponsored VASP continues to meet the necessary standards as required by VARA in respect of the VA Activities carried out by the Sponsored VASP; and
 - e. have adequate financial resources taking into account all business and/or VA Activities of all Sponsored VASPs.
2. Reporting. In addition to all reporting requirements in the other Rulebooks, Regulated Sponsors must provide VARA with the following information, in respect of each Sponsored VASP, on an annual basis—
 - a. complaints data;
 - b. full audited accounts; and
 - c. all other data as required by VARA from time to time.

Schedule 1 – Definitions

Term	Definition
“AML/CFT”	has the meaning ascribed to it in the Regulations.
“AML-CFT Report”	means all reports as required by the UAE FIU from time to time, including but not limited to— <ol style="list-style-type: none">(a) Suspicious Transaction Report (STR);(b) Suspicious Activity Report (SAR);(c) High Risk Country Transaction Report (HRC);(d) High Risk Country Activity Report (HRCA);(e) Funds Freeze Report; and(f) Partial Name Match Report.
“Anonymity-Enhanced Cryptocurrencies”	has the meaning ascribed to it in the Regulations.

“Anonymity-Enhanced Transactions”	means transactions denominated in Virtual Assets which are not Anonymity-Enhanced Cryptocurrencies, but which prevent the tracing of transactions or record of ownership.
“BCDR Plan”	means the Business Continuity and Disaster Recovery Plan of a VASP.
“Board”	has the meaning ascribed to it in the Company Rulebook.
“Capital and Prudential Requirements”	has the meaning ascribed to it in the Company Rulebook.
“CDD”	means client due diligence, including but not limited to due diligence on the clientele of a VASP’s client.
“Client Account”	has the meaning ascribed to it in <u>Part IV</u> of this Compliance and Risk Management Rulebook.
“Client Money”	has the meaning ascribed to it in <u>Part IV</u> of this Compliance and Risk Management Rulebook.
“Client VA”	has the meaning ascribed to it in <u>Part V</u> of this Compliance and Risk Management Rulebook.
“CMS”	means the compliance management system of a VASP.
“Compliance Officer” or “CO”	has the meaning ascribed to it in <u>Part I</u> of this Compliance and Risk Management Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means this Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Controlling Entity”	has the meaning ascribed to it in the Company Rulebook.
“Decentralised Autonomous Organisation” or “DAO”	has the meaning ascribed to it in the Company Rulebook.
“Directive”	has the meaning ascribed to it in the Regulations.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“EOCN”	means the UAE Executive Office for Control & Non-Proliferation.
“FATCA”	means the United States <i>Foreign Account Tax Compliance Act</i> .
“FATF”	means the Financial Action Task Force.
“Federal AML-CFT Laws”	has the meaning ascribed to it in the Regulations.
“Federal Competition Laws”	means <i>Federal Decree-Law No. (36) of 2023 Regulating Competition</i> , as may be in force from time to time, including all executive regulations, cabinet resolutions or cabinet decisions relating to the same, as may be published and/or amended from time to time.
“Fit and Proper Person”	means an individual who complies with all fit and proper requirements in the Company Rulebook.
“GoAML”	means the electronic platform through which Suspicious Transaction reports can be submitted to the UAE FIU.

“Group”	has the meaning ascribed to it in the Company Rulebook.
“Guidance”	has the meaning ascribed to it in the Regulations.
“Inside Information”	has the meaning ascribed to it in the Regulations.
“Insolvency Proceedings”	has the meaning ascribed to it in the Regulations.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Money Laundering Reporting Officer” or “MLRO”	has the meaning ascribed to it in Rule <u>III.A.1</u> of this Compliance and Risk Management Rulebook.
“Outsourcing”	has the meaning ascribed to it in the Company Rulebook.
“Paid-Up Capital”	has the meaning ascribed to it in the Company Rulebook.
“PDPL”	means the <i>Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data</i> .
“Personal Data”	has the meaning ascribed to it in the PDPL.
“Politically Exposed Person” or “PEP”	has the meaning ascribed to it in the Company Rulebook.
“Regulated Sponsor”	has the meaning ascribed to it in Rule VII.A of this Compliance and Risk Management Rulebook.
“Regulations”	means the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time.
“Related Parties”	has the meaning ascribed to it in the Company Rulebook.
“Reserve Assets”	has the meaning ascribed to it in the Company Rulebook.
“Responsible Individuals”	has the meaning ascribed to it in the Company Rulebook.
“Responsible Officer”	has the meaning ascribed to it in Rule <u>VII.G.1</u> of this Compliance and Risk Management Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Sponsored VASP”	has the meaning ascribed to it in Rule VII.A of this Compliance and Risk Management Rulebook.
“Staff”	has the meaning ascribed to it in the Company Rulebook.
“Suspicious Transaction”	<p>means any transaction, attempted transaction, or funds which a VASP has reasonable grounds to suspect as constituting, in whole or in part, and regardless of the amount or the timing, any of the following—</p> <ul style="list-style-type: none"> (a) the proceeds of crime (whether designated as a misdemeanour or felony, and whether committed within the Emirate or in another country in which it is also a crime); (b) being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organisations; and (c) being intended to be used in an activity related to such crimes.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to

	time.
“Third-Party Bank”	has the meaning ascribed to it in <u>Part IV</u> of this Compliance and Risk Management Rulebook.
“Travel Rule”	has the meaning ascribed to it in <i>FATF’s Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers</i> (October 2021), as may be amended from time to time.
“UAE”	means the United Arab Emirates.
“UAE FIU”	means the UAE Financial Intelligence Unit.
“Ultimate Beneficial Owner” or “UBO”	has the meaning ascribed to it in the Company Rulebook.
“UNSC”	means the United Nations Security Council.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VA Wallet”	has the meaning ascribed to the term “Virtual Asset Wallet” in the Dubai VA Law.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity Licensed by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.

Technology and Information Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Technology and Information Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out any VA Activity in the Emirate.

This Technology and Information Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out any VA Activity must also comply with the following Rulebooks applicable to all VASPs—

- Company Rulebook;
- Compliance and Risk Management Rulebook;
- Market Conduct Rulebook; and
- All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

Capitalised terms in this Technology and Information Rulebook have the meanings ascribed to them in the Regulations or as otherwise defined herein or provided in Schedule 2.

Unless otherwise stated, all requirements in this Technology and Information Rulebook are Rules and have binding effect.

Part I – Technology Governance, Controls and Security

A. Technology Governance and Risk Assessment Framework

1. VASPs must implement a technology governance and risk assessment framework, capable of determining defined policies underpinned by the necessary processes, procedures and controls that the VASP must implement, in order to adequately mitigate the risks identified (“**Technology Governance and Risk Assessment Framework**”).
2. VASPs must ensure that they implement all policies, processes, procedures and controls necessary to address risks to the VASP's business and VA Activities covered in the Technology Governance and Risk Assessment Framework using appropriate methods, including defence-in-depth approaches for cybersecurity-related risks. Such policies, processes, procedures and controls should take into account a number of factors including, the nature, scale and complexity of the VASP's business, the diversity of its operations, the volume and size of its transactions, and the level of risk inherent with its business.
3. The Technology Governance and Risk Assessment Framework must be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in the VASP's business model and VA Activities. The Technology Governance and Risk Assessment Framework should apply to all technologies relevant to a VASP's business and VA Activities and clearly set out—
 - a. the VASP's cybersecurity objectives, including the requirements for the competency of Staff and, as relevant, end users and clients; and
 - b. clearly defined policies, processes, procedures and controls necessary for managing risks, including, but not limited to, consideration of international standards and industry best practice codes.
4. VASPs must ensure that their Technology Governance and Risk Assessment Framework addresses appropriate governance policies and system development controls, including but not limited to—
 - a. a development, maintenance and testing process for technology systems;
 - b. operations controls;
 - c. back-up controls;
 - d. capacity and performance planning; and
 - e. availability testing.
5. VASPs must monitor, assess and maintain the effectiveness of their Technology Governance and Risk Assessment Framework. In particular, VASPs must review, update and arrange for the testing of their policies, processes, procedures and controls aimed at managing risks on a periodic basis, having regard to the macroeconomic environment in which the VASP operates, as well as emerging technology risks relating to their systems and consideration of international standards and industry best practice codes.
6. VARA has provided Guidance, in Schedule 1 of this Technology & Information Rulebook, on the categories of risk, the risk mitigation measures and standards that a VASP's Technology Governance and Risk Assessment Framework should cover when complying with the Rules in this Part I of the Technology & Information Rulebook.
7. As prescribed by Rule I.I.1 of this Technology and Information Rulebook, VASPs must appoint a Chief Information Security Officer who is responsible for ensuring that the VASP complies with

Part I and Part III of this Technology and Information Rulebook.

B. Cybersecurity Policy

1. VASPs must create and implement a policy which outlines their procedures for the protection of their electronic systems and client and counterparty data stored on those systems (“**Cybersecurity Policy**”). VASPs must submit their Cybersecurity Policy to VARA for assessment as part of the licensing process and at any subsequent time upon request from VARA.
2. VASPs must ensure that their Cybersecurity Policy is reviewed and updated at least annually by their CISO.
3. VASPs must ensure that their Cybersecurity Policy contains sound procedures and security mechanisms in accordance with best industry practices that will enable them to comply with all applicable information security, data protection and data privacy laws and regulations, including but not limited to Part II of this Technology and Information Rulebook and the PDPL, whilst maintaining the confidentiality of data at all times. The Cybersecurity Policy must address the following minimum criteria—
 - a. information security;
 - b. data governance and classification;
 - c. access controls;
 - d. capacity and performance planning;
 - e. systems operations and availability concerns;
 - f. systems and network security, consensus protocol methodology, code and smart contract validation and audit processes;
 - g. systems and application development and quality assurance;
 - h. physical security and environmental controls, including but not limited to procedures around access to premises and systems;
 - i. procedures regarding their facilitation of Virtual Asset transactions initiated by a client including, but not limited to, considering multi-factor authentication or any better standard for Virtual Asset transactions that—
 - i. exceed transaction limits set by the client, such as accumulative transaction limits over a period of time; and
 - ii. are initiated after a change of personal details by the client, such as the address of a VA Wallet;
 - j. procedures regarding client authentication and session controls including, but not limited to, the maximum incorrect attempts for entering a password, appropriate time-out controls and password validity periods;
 - k. procedures establishing adequate authentication checks when a change to a client’s account information or contact details is requested;
 - l. in addition to all applicable requirements in Part II of this Technology and Information Rulebook, client data privacy, including but not limited to—
 - i. the security and authentication of the means of transfer of information;
 - ii. the minimisation of the risk of data corruption and unauthorised access to data; and
 - iii. the prevention of information leakage;

- m. vendor and third-party service provider management;
- n. monitoring and implementing changes to core protocols not directly controlled by the VASP, as applicable;
- o. incident response, including but not limited to root cause analysis and rectification activities to prevent reoccurrence;
- p. supplier probity and Staff vetting procedures;
- q. governance framework and escalation procedures for effective decision-making and proper management and control of risks and emergency incidents, including but not limited to responses to ransomware and other forms of cyberattacks; and
- r. hardware and infrastructure standards, including but not limited to network lockdown, services/desktop security and firewall standards; and
- s. sharing cyber threat information and intelligence with other VASPs and/or Entities—
 - i. whenever such action is in the best interests of the Virtual Asset market as a whole, to enhance operational resilience, manage the threat and, where practicable, minimise and/or mitigate the impact of such threat; and provided that, sharing such information does not increase any risks to the VASP and/or mandate the exposure of confidential information relating to the VASP sharing such information.
 - ii.

C. Cybersecurity – other Legal and Regulatory Obligations

1. VASPs must ensure that their Technology Governance and Risk Assessment Framework complies with, to the extent applicable, cybersecurity laws, regulatory requirements and guidelines, including but not limited to—
 - a. the electronic security requirements and standards adopted by the Dubai Electronic Security Center per *Law No. (9) of 2022 Regulating the Provision of Digital Services Provided in the Emirate of Dubai*;
 - b. the *Federal-Decree Law No. (45) of 2021 on the Protection of Personal Data*, its executive regulations and any other cybersecurity regulatory requirements as may be imposed by the UAE Data Office from time to time; and
 - c. the *Consumer Protection Regulation* issued pursuant to *Central Bank Notice No. (444) of 2021* and any other cybersecurity regulatory requirements as may be imposed by the CBUAE from time to time.

D. Cryptographic Keys and VA Wallets Management

1. VASPs must ensure that their Technology Governance and Risk Assessment Framework addresses, to the extent necessary, the generation of cryptographic keys and VA Wallets, the signing and approval of transactions, the storage of cryptographic keys and seed phrases, VA Wallet creation and management thereof.
2. VASPs must—
 - a. safeguard access to Virtual Assets in accordance with industry best practices and, in particular, ensure that there is no single point of failure in the VASP's access to, or knowledge of, Virtual Assets held by the VASP;

- b. adopt industry best practices for storing the private keys of clients, including ensuring that keys stored online or in any one physical location are insufficient to conduct a Virtual Asset transaction, unless appropriate controls are in place to render physical access insufficient to conduct such Virtual Asset transaction. VASPs must further ensure that backups of the key and seed phrases are stored in a separate location from the primary key and/or seed phrase;
- c. adopt strict access management controls to manage access to keys, including an audit log detailing each change of access to keys. In particular, if Staff with access to a key (including a multi-signature arrangement key) leaves the employment of that VASP, the VASP must conduct an assessment to determine whether a new key must be generated;
- d. adopt procedures designed to immediately revoke a key signatory's access. In particular, a VASP must—
 - i. ensure that the key generation process ensures that revoked signatories do not have access to the backup seed phrase or knowledge of the phrase used in the key's creation;
 - ii. perform internal audits on a quarterly basis concerning the removal of user access by reviewing access logs and verifying access as appropriate;
 - iii. implement and maintain a procedure for documenting the onboarding and offboarding of Staff;
 - iv. implement and maintain a procedure for documenting a VASP's permission to grant or revoke access to each role in its key management system; and
- e. regularly assess the security of their information technology systems or software integrations with external parties and ensure that the appropriate safeguards are implemented in order to mitigate all relevant risks.

3. VASPs should provide information to clients on measures they can take to protect their keys and/or seed phrases from misuse or unauthorised access, and the consequences of sharing their private keys and other security information.
4. VASPs must ensure that access to their systems and data may only be granted to individuals with a demonstrable business need and implement safeguards to ensure the proper identification of all individuals, including the maintenance of an access log.

E. Testing and Audit

1. VASPs must engage a qualified and independent third-party auditor to conduct vulnerability assessments and penetration testing (including, to the extent relevant to the VASP's business and VA Activities, comprehensive audits of the effectiveness, enforceability and robustness of all smart contracts) at least on an annual basis and prior to the introduction of any new systems, applications and products. VASPs must provide the results of any such assessments and tests to VARA upon VARA's request.
2. VASPs should maintain effective internal functions and measures for continuous monitoring of their operations and processes. In particular, on a regular basis and on request by VARA, VASPs must perform—
 - a. security testing on both infrastructure and applications; and
 - b. internal system and external system vulnerability audits.

3. Evidence of tests and audits must be documented by VASPs and made immediately available by them for inspection by VARA, upon VARA's request.
4. VASPs shall ensure that they are regularly audited by independent auditors to examine their management processes for ensuring the effectiveness of their processes, procedures and controls, and their compliance with regulatory requirements. VASPs must provide the results of any such audit to VARA upon VARA's request.
5. VARA may notify a VASP that it is required to carry out advanced testing by means of TLPT, where VARA considers it necessary and proportionate to do so, taking into account the following factors—
 - a. any specific risks to which a VASP is or might be exposed;
 - b. the criticality of a VASP's business and/or VA Activities; and
 - c. any other relevant risks.
6. All TLPTs required under Rule I.E.5 must be carried out in accordance with the following conditions—
 - a. each TLPT is to be carried out by an external tester;
 - b. TLPTs may be required by VARA to cover Critical or Important Functions of a VASP and, where required, be performed on live production systems, technologies and processes supporting such Functions;
 - c. where it is necessary for third-party service providers of the VASP to be included in the scope of a TLPT, the VASP shall ensure the participation of such third-party service providers in the TLPT;
 - d. VASPs shall mitigate the risks of testing including any potential impact on data, damage to assets, and disruption to Critical or Important Functions, services or operations at the VASP itself or to counterparts, and with due security assurance of data and privacy of client assets;
 - e. at the end of the testing, the VASP (together with the external tester) shall produce a summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with all relevant requirements as stated herein; and
 - f. the VASP shall promptly provide all documentation relating to the TLPT to VARA, including the summary of the relevant findings, the remediation plans and the documentation demonstrating that the TLPT has been conducted in accordance with all relevant requirements as stated herein.
7. VASPs must ensure that the external testers they use to carry out any TLPT—
 - a. are suitable and of good repute;
 - b. possess all necessary technical and organisational capabilities and demonstrate specific expertise in threat intelligence and penetration testing;
 - c. are certified by an accreditation body, or adhere to formal codes of conduct or ethical frameworks;
 - d. provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of the TLPT, including the due protection of the VASP's confidential information; and
 - e. are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.

8. VASPs shall ensure that contracts concluded with external testers—
 - a. require sound management of the TLPT results and any data processing thereof, including any generation, storage, aggregation, draft, report, communication or destruction; and
 - b. do not create additional risks for the VASP or any of its systems.
9. Third-party technology service providers. Where the participation of a third-party technology service provider is required in any TLPT, as referred to in Rule I.E.6.c, the VASP and the third-party technology service provider may agree that such third-party technology service provider directly enters into contractual arrangements with the external tester appointed by the VASP under Rule I.E.6.a, if such participation is reasonably expected to have an adverse impact on—
 - a. the quality or security of services delivered by such third-party technology service provider to the market; or
 - b. on the confidentiality of the data related to such services.
10. In the event that a third-party technology service provider directly enters into contractual arrangements with the external tester appointed by the VASP for a TLPT under Rule I.E.9, the VASP notified by VARA to carry out the TLPT must ensure that—
 - a. the third-party technology service provider remains under the direction of the VASP;
 - b. the results shall cover the relevant range of services supporting Critical or Important Functions of the VASP notified by VARA; and
 - c. all results provided by the third-party technology service provider to the external tester must be a fair representation of, and specific to, the VASP.

F. Virtual Asset Transactions

1. VASPs must implement controls that prevent the manipulation or coordinated collusion or attacks of automated systems.
2. In addition to all applicable requirements in the Compliance and Risk Management Rulebook, VASPs must implement and maintain distributed ledger tracing software to screen incoming and outgoing Virtual Asset transactions and VA Wallet addresses. How VASPs will respond to any Suspicious Transactions must be set out in their AML/CFT policies in accordance with the Compliance and Risk Management Rulebook.

G. Algorithm Governance

1. If a VASP conducts VA Activities using algorithms (in whole or in part), it must establish policies and procedures that enable its Board and Senior Management to have robust oversight and control over the design, testing, performance, deployment and ongoing maintenance of such algorithms.
2. VASPs must maintain documentation and records of the design, testing, performance, deployment and ongoing maintenance of such algorithms, including but not limited to the logic used by the algorithm, any data or assumptions upon which decisions are based and any potential or actual biases in such data or assumptions and any results produced by the algorithm.
3. VASPs must ensure that they have qualified and competent Staff to ensure the proper functioning and supervision of such algorithms on an ongoing basis.

H. Business Continuity, Cybersecurity Events and Risk

1. VASPs must implement, maintain, test and update on an annual basis an adequate Business Continuity and Disaster Recovery Plan (“**BCDR Plan**”) to minimise disruption to their operations. The BCDR Plan must address, but not be limited to—
 - a. events that may trigger the implementation of the BCDR Plan, such as cybersecurity events and technical failures, and procedures to be taken to assess the nature, scope and impact of the event;
 - b. resource requirements, including but not limited to Senior Management and Staff, systems and other assets;
 - c. recovery priorities for the VASP’s operations, including but not limited to the preservation of essential data and critical functions and the maintenance of those data and functions;
 - d. communication arrangements for affected internal and external parties;
 - e. processes to validate the integrity of information affected by any interruption;
 - f. procedures to mitigate operational impact and/or to transfer operational functions including, but not limited to, escalation of response and recovery activities to designated personnel and management;
 - g. an alternative site sufficient to recover and continue operations for a reasonable period; and
 - h. procedures to remediate identified and/or exploited vulnerabilities or upgrade relevant protocols once stable operations are resumed to prevent similar events.
2. The BCDR Plan should take into consideration and address factors and issues specific to Virtual Assets and DLT including, but not limited to, network malfunction, loss of data or compromise in data integrity, and key storage and maintenance of authorisation layers.

I. Chief Information Security Officer and Management

1. VASPs must appoint a Chief Information Security Officer (“**CISO**”) who is responsible for ensuring that the VASP complies with Part I and Part III of this Technology and Information Rulebook. The CISO must be a separate individual from the CO however the CISO may also take on the responsibilities of the Data Protection Officer under Rule II.B.2 of this Technology and Information Rulebook.
2. The CISO must be of sufficiently good standing and appropriately experienced.
3. Senior Management must regularly assess and review the effectiveness of the VASP’s processes, procedures and controls in relation to the VASP’s compliance with this Technology and Information Rulebook and all applicable laws and regulatory requirements, as well as allocate duties and apportion roles and responsibilities within the VASP to prevent conflicts of interests.

J. Staff Competency

1. In addition to relevant requirements in the Compliance and Risk Management Rulebook, VASPs must ensure that all Staff are aware of the latest cybersecurity risks and developments (including those specific to Virtual Assets and DLT), taking into account the type and level of cyber risks that they may face in their respective roles.

K. Notification to VARA

1. In addition to relevant requirements in the Compliance and Risk Management Rulebook, upon the detection of any occurrence of (i) a material cybersecurity event or (ii) an event triggering the implementation of the BCDR Plan that materially impacts a VASP's business operations, the VASP shall report such event to VARA as soon as reasonably practicable, and in any event no later than seventy-two (72) hours from detection, with all relevant details of the nature, scope and impact of such event and the steps the VASP is or will be taking to mitigate such impact including, but not limited to, whether any notifications or reports have been made to authorities other than VARA.

Part II – Personal Data Protection

A. Compliance with Applicable Data Protection Law

1. VASPs must comply with all applicable data protection and data privacy requirements in all relevant jurisdiction(s) as follows—
 - a. within the UAE, including the PDPL and any sectoral or free zone laws and regulations that may apply to the VASP; and
 - b. any data protection laws outside of the UAE that may apply to the VASP's activities wheresoever conducted.
2. Compliance with all applicable data protection and data privacy requirements under Rule II.A.1 of this Technology and Information Rulebook shall include, but not be limited to, where data may be stored or located and how such data is transferred.

B. Compliance Programme

1. VASPs shall produce and implement a written compliance programme to protect the privacy of Personal Data, in accordance with all applicable data protection laws.
2. Notwithstanding the requirements of any applicable data protection laws, VASPs shall at a minimum comply with the following VARA requirements—
 - a. appoint a Data Protection Officer who has the appropriate competencies and experience to perform the statutory duties and responsibilities associated with this role under applicable data protection laws (including under Article 11 of the PDPL) (“**Data Protection Officer**”). The Data Protection Officer can be the same individual as the CISO of the VASP; and
 - b. establish a function in their organisation that is responsible for the management and protection of Personal Data in accordance with all applicable law and is appropriate for the level of risk involved with such Personal Data, including responsibility for implementing and maintaining appropriate processes, procedures and controls.

C. Provision of Information to VARA

1. Notwithstanding any other requirement elsewhere in the Regulations, Rulebooks or Directives, VASPs shall take all steps, including where applicable provide all notifications, contractual provisions and obtain all consents, that are necessary to enable VARA to have access to any

information relating to the VASP's compliance with this Part II of this Technology and Information Rulebook, regardless of where such information is stored. Access to such information shall be provided by VASPs in the manner and within the timelines communicated by VARA to the VASP.

2. VASPs shall notify VARA as soon as possible and in any event within twenty-four (24) hours following notification by them to either—

- a. any data regulator, including in the UAE; or
- b. a Data Subject

of any incident affecting, or potentially affecting, Personal Data and shall provide VARA with a summary of such report and, where the relevant data regulator is located in the UAE, a copy of such report, unless and to the extent prohibited by applicable law as demonstrated by the VASP to VARA's satisfaction.

Part III – Confidential Information

A. Use and Protection of Confidential Information by VASPs

1. VASPs shall take all reasonable steps to protect the ongoing confidentiality of all information related to their clients and all related properties and records. Such steps shall include implementing and enforcing appropriate policies, procedures and mechanisms to protect the confidential nature of any information shared with them, whether under the terms of a confidentiality agreement or otherwise.
2. Such policies, procedures and mechanisms shall require that use of any information related to a VASP's clients is only made for the purposes for which the information is provided and in compliance with relevant confidentiality agreements which shall be consistent with applicable laws and regulatory requirements, including with respect to acceptance of such agreements.
3. VASPs shall—
 - a. familiarise Staff with—
 - i. their internal policies on the collection and processing of confidential information; and
 - ii. requirements in this Part III of this Technology and Information Rulebook as applicable to relevant Staff; and
 - b. periodically certify their Staffs' compliance with such internal policies.
4. Staff must not share confidential information within the VASP or with any other Entities unless it is absolutely necessary for the purposes of conducting VA Activities related to such confidential information.
5. Neither VASPs nor their Staff shall use or share confidential information for the purpose of the trading of Virtual Assets by any Entity.

Schedule 1 – Guidance on Technology Governance and Risk Assessment Frameworks

Introduction

All VASPs are required to implement a Technology Governance and Risk Assessment Framework under Rule I.A.1 of this Technology and Information Rulebook. This Schedule 1 is provided by VARA as Guidance to VASPs, to assist them in creating effective Technology Governance and Risk Assessment Frameworks.

VASPs should consider all categories of risk and the risk mitigation standards (as may be applicable), set out in this Schedule 1 of the Technology & Information Rulebook, when creating their Technology Governance and Risk Assessment Frameworks.

Nothing in this Schedule 1 of the Technology & Information Rulebook shall limit, reduce or otherwise amend any Rules, or other requirements, with which VASPs must comply, under any applicable laws or regulations, Regulations, Rules or Directives, including but not limited to in respect of Personal Data protection.

A. Risk Category 1: Organisational

1. Comprehensive security framework standard: VASPs are expected to utilise a balanced approach to ensure that security resources are allocated appropriately across their entire organisation, preventing security gaps and minimising single points of failure that attackers can exploit. VASPs are expected to implement a documented security framework that addresses both wallet infrastructure and enterprise security. The framework is expected to include, but not be limited to —
 - a. regular security assessments of all system components;
 - b. formal risk assessment methodology, including risks inherent in both centralised and decentralised structures;
 - c. governance structure with clear security accountability; and
 - d. adoption of best in class standards.
2. Secure development lifecycle standard: To ensure that security is integrated throughout the development process, reducing the accumulation of security debt even in rapid development environments, VASPs are expected to establish and adhere to a formal secure development lifecycle methodology that incorporates security at every stage, from requirements gathering to deployment and maintenance. This methodology is expected to include, but not be limited to—
 - a. defining security requirements and mandatory security review gates before deployment;
 - b. threat modelling for new features and secure coding standards; and
 - c. post-implementation validation of the efficacy of the measures deployed.
3. Workforce security management standard: To address the unique challenges of the distributed workforce model common in the VA space, and to reduce the risk of compromised developer workstations leading to system intrusions, VASPs are expected to implement comprehensive workforce security controls, including but not limited to—
 - a. mandatory endpoint protection for all devices with access to any systems, including but not limited to production systems;
 - b. regular security awareness training specific to common threats;
 - c. background checks for all personnel with access to sensitive or critical systems;
 - d. formalised onboarding and offboarding procedures for all staff, including contractors; and

- e. minimum security requirements for personal devices used for work purposes.
- 4. Infrastructure management standard: To ensure visibility across dispersed infrastructure, reducing security gaps at environment boundaries and enabling effective security monitoring, VASPs are expected to maintain comprehensive infrastructure documentation and controls, including but not limited to—
 - a. comprehensive asset inventories across all environments;
 - b. network diagrams and data flow mappings;
 - c. centralised configuration management and formal change control processes; and
 - d. regular infrastructure security assessments.
- 5. Third-party technology service provider standard: To ensure risks arising from the use of third-party technology services are incorporated as part of the VASP's framework, VASPs are expected to implement appropriate standards and controls for each third-party technology service provider, which are proportionate to the nature, scale, complexity and importance of the services provided, including but not limited to—
 - a. conducting comprehensive due diligence on all such service providers;
 - b. having in place written contractual arrangements with all such service providers; and
 - c. adopting multi-vendor strategies where possible and/or practicable.

B. Risk Category 2: Technical

- 1. Key generation standard: To reduce the risk of weak or predictable keys that could be exploited by attackers, VASPs are expected to generate cryptographic keys using industry-approved methods with sufficient entropy, including but not limited to—
 - a. hardware security modules (“**HSMs**”) for key generation, where possible;
 - b. formal validation of key generation routines;
 - c. best in class security processes for all cryptographic keys, including minimum standards for encryption;
 - d. separation of duties during key generation; and
 - e. comprehensive audit logging of all generation activities.
- 2. Wallet creation standard: To ensure that wallets are created in a controlled, secure environment with appropriate oversight, VASPs are expected to implement a secure wallet creation process that includes, but is not limited to—
 - a. formal wallet creation procedures with separation of duties;
 - b. multiple levels of approval for new wallet creation;
 - c. tamper-evident processes for all creation activities;
 - d. comprehensive logging and monitoring of wallet creation; and
 - e. physical security controls for creation environments.
- 3. Key storage security standard: To reduce the risk of key compromise, which is the most direct path to asset theft, VASPs are expected to store cryptographic keys using defence-in-depth

approaches, including but not limited to—

- a. HSMs for critical key storage;
- b. appropriate separation of key components for keys-at-rest including both physical decentralisation and encryption/cryptographic methods;
- c. restricted physical and logical access to key storage mechanisms; and
- d. regular testing of key backup and recovery procedures.

4. Smart contract security standard: To reduce the risk of vulnerabilities in smart contract code that could be exploited to manipulate transactions or extract funds, VASPs are expected to implement formal smart contract review and testing processes, including but not limited to—

- a. static and dynamic code analysis;
- b. independent third-party audits before deployment and formal verification where applicable;
- c. comprehensive penetration testing; and
- d. regular re-assessment of deployed contracts.

5. Multi-signature security standard: To eliminate single points of failure in wallet security and ensure resilience against compromise of individual signers, VASPs are expected to implement robust multi-signature requirements, including—

- a. minimum multi-signatures for high-value operations, where the minimum number of signers (M) is greater than the total number of signatories (N) divided by two (2) (i.e. $M > N/2$);
- b. geographic distribution of signing authorities;
- c. diverse authorisation mechanisms and separation of duties between signers; and
- d. regular testing of signature processes.

6. Transaction verification standard: To reduce the risk of authorising fraudulent transactions, VASPs are expected to implement comprehensive transaction verification processes, including but not limited to—

- a. mandatory multi-level verification;
- b. automated detection of anomalous transactions in real-time triggering immediate notifications;
- c. clear procedures for signers to verify and validate transactions;
- d. formal process for addressing verification anomalies; and
- e. immediate halting of the signing process when errors are reported.

7. Key compromise response standard: To ensure organisations can respond effectively to suspected or confirmed key compromises and to limit potential damage, VASPs are expected to develop and maintain a formal key compromise response plan that includes, but is not limited to

- a. clear triggers for activation, with pre-authorised emergency response procedures and formal communication protocols;
- b. rapid key rotation capabilities; and
- c. regular testing and simulation.

8. Key holder management standard: To reduce the risk of unauthorised access to cryptographic keys through proper lifecycle management of key holders, VASPs are expected to implement comprehensive key holder management processes, including but not limited to—
 - a. just-in-time access provisioning;
 - b. regular access reviews and immediate revocation processes;
 - c. segregation of duties; and
 - d. secure backup key holder procedures.
9. Authentication control standard: To reduce the risk of unauthorised access through comprehensive authentication requirements, VASPs are expected to implement strong authentication controls, including but not limited to—
 - a. multi-factor authentication for all access to systems with cryptographic keys;
 - b. hardware-based authentication for critical operations, with biometric verification where appropriate;
 - c. time-based restrictions on authentication attempts; and
 - d. continuous validation of session authenticity.
10. Developer workstations standard: To address a common initial access vector for attackers by securing the development environment, VASPs are expected to implement strict controls for developer workstations, including but not limited to—
 - a. endpoint protection and monitoring;
 - b. network segmentation;
 - c. prohibition of direct production access;
 - d. secure secret management solutions; and
 - e. regular security assessments.
11. Security testing standard: To ensure ongoing identification and remediation of vulnerabilities before they can be exploited, VASPs are expected to conduct appropriate security tests regularly, and in all events prior to any update to a production system. Such security test should include, but not be limited to—
 - a. annual penetration testing by qualified third parties;
 - b. quarterly vulnerability assessments;
 - c. continuous automated security scanning;
 - d. regular best practice security exercises for high-value systems; and
 - e. formal remediation tracking for identified vulnerabilities.
12. Unauthorised recovery standard: To reduce the risk of unauthorised recovery of cryptographic keys from disposed media, VASPs are expected to implement comprehensive data sanitisation policies and procedures that ensure—
 - a. secure disposal of all media containing sensitive information;
 - b. cryptographic erasure or physical destruction of media containing cryptographic keys;
 - c. formal chain of custody documentation for media disposal;
 - d. regular assessment of sanitisation effectiveness; and

- e. secure decommissioning procedures for all systems.

13. Audit logging standard: To enhance visibility into system activities and support effective investigation of security incidents, VASPs are expected to implement comprehensive monitoring and logging systems that—

- a. capture all security-relevant events and store logs securely with tamper-evidence, maintaining logs for a minimum of one year;
- b. include all wallet and key operations; and
- c. implement real-time alerting for security events.

C. Risk Category 3: Detection and Response

- 1. Transaction monitoring standard: To enable early detection of fraudulent activities, VASPs are expected to implement comprehensive transaction monitoring, including but not limited to—
 - a. behavioural analysis to detect anomalous patterns, and rule-based monitoring for known suspicious activities;
 - b. machine learning capabilities for advanced threat detection;
 - c. real-time alerting for Suspicious Transactions; and
 - d. regular review and refinement of detection methodologies.
- 2. Internal user activity monitoring standard: To enhance the ability to identify compromised accounts or insider threats early, VASPs are expected to implement monitoring of internal user activities, including but not limited to—
 - a. authentication attempts and failures and pattern analysis to detect insider threats;
 - b. access to sensitive or critical systems and administrative activities; and
 - c. segregation of monitoring from operational teams.
- 3. Enhanced monitoring standard: To provide visibility into activities on critical systems, enabling early detection of any compromises, VASPs are expected to implement enhanced monitoring of developer and signing systems, including but not limited to—
 - a. process creation and termination monitoring;
 - b. network connection analysis and file system change detection;
 - c. software installation and execution control; and
 - d. user behaviour analytics.
- 4. Tactical hardening standard: To enable organisations to limit attacker access once a compromise is detected, VASPs are expected to maintain capability to rapidly implement tactical hardening measures, including but not limited to—
 - a. emergency access revocation, including individual end-points;
 - b. network segmentation capabilities and system isolation procedures;
 - c. pre-approved emergency change procedures; and
 - d. regular testing of hardening capabilities.

5. Investigation capability standard: To enhance the ability to identify attack vectors and compromised assets during incidents, VASPs are expected to maintain comprehensive investigation capabilities, including but not limited to—
 - a. dedicated forensic resources (internal or contracted) deployable and responsive in real-time and/or on immediate notice;
 - b. secure evidence collection and handling procedures;
 - c. chain of custody documentation;
 - d. root cause analysis methodologies; and
 - e. regular training and capability testing.
6. On-chain analysis standard: To improve the ability to trace stolen funds and identify potential recovery opportunities, VASPs are expected to develop and maintain on-chain analysis capabilities, including but not limited to—
 - a. transaction tracing tools and wallet attribution capabilities;
 - b. collaboration with other VASPs for fund tracing; and
 - c. regular training and capability development.
7. Remediation standard: To reduce the risk of re-exploitation, VASPs are expected to implement comprehensive remediation procedures, including but not limited to—
 - a. complete rotation of all secret components (including but not limited to passwords, keys and key shards) after incidents;
 - b. system rebuilding from secure baselines and enhanced monitoring post-incident;
 - c. formal verification of attacker removal; and
 - d. post-incident review and lessons learned.

D. Risk Category 4: Customer VAs

1. Customer authentication standard: To reduce the risk of any customer account compromises, VASPs are expected to implement robust customer authentication, including but not limited to—
 - a. strong multifactor authentication;
 - b. prohibition of instant messaging verification for high-risk operations;
 - c. risk-based authentication challenges and biometric authentication where appropriate; and
 - d. suspicious login detection and alerting.
2. Withdrawal control standard: To limit potential losses from compromised accounts through structured withdrawal controls, VASPs are expected to implement comprehensive withdrawal controls, including—
 - a. tiered withdrawal limits;
 - b. cooling periods for large transactions;
 - c. verification for high-value withdrawals outside of prescribed limits and/or 'bands';
 - d. verification for critical transactions;
 - e. behavioural analysis to detect anomalous withdrawal patterns; and

- f. graduated approval requirements based on transaction value.
- 3. User education standard: To reduce customer vulnerability to social engineering and other attacks through improved awareness, VASPs are expected to implement comprehensive user education programmes, including but not limited to—
 - a. security best practices;
 - b. common attack vector awareness and secure account management guidance; and
 - c. regular security notifications.
- 4. VA Wallet concentration risk standard: To reduce the risk of concentration of Client VAs in a single or small number of VA Wallets, VASPs are expected to implement controls for the safe diversification of Client VAs across VA Wallets, including but not limited to—
 - a. cold storage VA Wallets;
 - b. VARA Licensed VASPs providing Custody Services; and
 - c. physical distribution of servers storing information through which VA Wallets can be accessed and/or controlled.

E. Risk Category 5: Digital Operational Resilience

- 1. Digital operational resilience test standard: To achieve a high level of digital operational resilience, VASPs are expected to carry out digital operational resilience testing including, but not limited to—
 - a. establishing and maintaining a sound and comprehensive digital operational resilience testing programme, including a range of assessments, tests, methodologies, practices and tools as set out below in paragraph 2;
 - b. identifying weaknesses, deficiencies and gaps in digital operational resilience and promptly implementing corrective measures;
 - c. when conducting the digital operational resilience testing programme, VASPs should follow a risk-based approach taking into account any specific risks to which the VASP is or might be exposed, the criticality of assets and of services provided by or to the VASP, as well as any other material risk factor;
 - d. ensuring that tests are undertaken by independent external parties;
 - e. classifying and remedying all issues revealed throughout the performance of the tests and establishing internal validation processes to ascertain that all identified weaknesses, deficiencies or gaps are fully addressed; and
 - f. ensuring that appropriate tests are conducted at least yearly on all systems and applications supporting Critical or Important Functions.
- 2. The digital operational resilience testing programme referred to in paragraph 1 should provide for testing of tools and systems through the execution of appropriate tests, including but not limited to—
 - a. vulnerability assessments and scans;
 - b. open source analyses;
 - c. network security assessments;
 - d. gap analyses;

- e. physical security reviews;
- f. questionnaires and scanning software solutions;
- g. source code reviews;
- h. scenario-based tests;
- i. compatibility testing;
- j. performance testing;
- k. end-to-end testing; and
- l. penetration testing.

Schedule 2 – Definitions

Term	Definition
“AML/CFT”	has the meaning ascribed to it in the Regulations.
“BCDR Plan”	has the meaning ascribed to it in Rule <u>I.H.1</u> in this Technology and Information Rulebook.
“Board”	has the meaning ascribed to it in the Company Rulebook.
“CBUAE”	means the Central Bank of the United Arab Emirates.
“Chief Information Security Officer” or “CISO”	has the meaning ascribed to it in Rule <u>I.I.1</u> of this Technology and Information Rulebook.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance Officer” or “CO”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Critical or Important Function”	has the meaning ascribed to it in the Company Rulebook.
“Cybersecurity Policy”	has the meaning ascribed to it in Rule <u>I.B.1</u> in this Technology and Information Rulebook.
“Data Protection Officer” or “DPO”	has the meaning ascribed to it in Rule <u>II.B.2</u> of this Technology and Information Rulebook.
“Data Subject”	has the meaning ascribed to it in the PDPL.
“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to the term “Distributed Ledger Technology” in the Dubai VA Law.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Function”	has the meaning ascribed to it in the Company Rulebook.
“Guidance”	has the meaning ascribed to it in the Regulations.
“HSM”	means a hardware security module.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“PDPL”	means the <u>Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data</u> .

“Personal Data”	has the meaning ascribed to it in the PDPL.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Staff”	has the meaning ascribed to it in the Company Rulebook.
“Suspicious Transactions”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Technology and Information Rulebook”	means this Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Technology Governance and Risk Assessment Framework”	has the meaning ascribed to it in Rule I.A.1 of this Technology and Information Rulebook.
“Threat Led Penetration Testing” or “TLPT”	means a framework that mimics the tactics, techniques and procedures of real- life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the VASP's critical live production systems.
“UAE”	means the United Arab Emirates.
“UAE Data Office”	means the UAE Data Office established by virtue of <i>Federal Decree-Law No. (44) of 2021 Establishing the UAE Data Office</i> .
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VA Wallet”	has the meaning ascribed to the term “Virtual Asset Wallet” in the Dubai VA Law.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity Licensed by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.

Market Conduct Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Market Conduct Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out any VA Activity in the Emirate.

This Market Conduct Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out any VA Activity must also

comply with the following Rulebooks applicable to all VASPs—

- Company Rulebook;
- Compliance and Risk Management Rulebook;
- Technology and Information Rulebook; and
- All Rulebooks specific to the VA Activities that the VASP is Licensed by VARA to carry out.

Capitalised terms in this Market Conduct Rulebook have the meanings ascribed to them in the Regulations or as otherwise defined herein or provided in Schedule 1.

Unless otherwise stated, all requirements in this Market Conduct Rulebook are Rules and have binding effect.

Part I – Marketing, Advertising and Promotions

A. Marketing Regulations

1. VASPs must comply with the Marketing Regulations, at all times.

Part II – Client Agreements

A. Requirement for Written Agreements

1. VASPs shall enter into written agreements with each client which specify the VASP's duties and responsibilities when providing services including all VA Activities (“**Client Agreements**”).
2. VASPs must comply with Client Agreements at all times.
3. VASPs must ensure that, in addition to all applicable laws, including but not limited to consumer protection laws, all Client Agreements comply with the general requirement for the VASP to act honestly, fairly and in the best interests of its clients and the integrity of the market.
4. Client Agreements must at all times be fair, clear, transparent, accurate and not misleading. Client Agreements must be sufficiently clear to the client, having regard to the nature of the services and the intended market for such services.
5. VASPs must obtain valid acceptance from all clients entering into Client Agreements, which must be given in a form which is compliant with all applicable laws and prior to the VASP providing any VA Activities to the client.
6. VASPs must send a copy of the Client Agreement to each client after it has been entered into.
7. VASPs must notify clients of any change to Client Agreements at least thirty (30) calendar days prior to any change taking effect.
8. If VASPs have the right in any Client Agreement to be able to unilaterally change a service, or any part of a service, or VA Activity, this must be made explicit in the Client Agreement.
9. VASPs must maintain a record of all versions of Client Agreements and be able to identify all changes made between versions.

B. Content of Client Agreements

1. Client Agreements shall include, but not be limited to—

- a. the identities of the client and the VASP, including the legal name and registered address of the VASP;
- b. a description of the VASP's Group;
- c. a description of the services to be provided;
- d. the methods that the VASP and client will use to communicate regarding the services;
- e. all fees charged by the VASP for the services;
- f. the law applicable to the Client Agreement;
- g. identification of third-party service providers, or any Entities within the VASP's Group, utilised by the VASP and necessary for the services provided under the Client Agreement, which may be provided in the form of a description of the services they perform;
- h. clearly identify if and when any Virtual Assets are no longer under the control of the VASP during the provision of any VA Activity, and describe the Entity(ies) liable for Virtual Assets at all times, including but not limited to where such Entity(ies) are located;
- i. a clear statement that neither Client VAs nor Client Money benefit from any form of deposit protection;
- j. a clear statement that all client assets, including but not limited to Client Money and Client VAs, remain owned by the client; and
- k. clearly identify if and when any assets, including but not limited to money or Virtual Assets, will not be owned by the client at any time.

2. When forming Client Agreements, VASPs must also consider and include to the extent applicable to the services being provided, provisions covering the following—
 - a. specification of what Virtual Assets are, or will be, supported;
 - b. a description of how the VASP will respond to newly created Virtual Assets (e.g. from an 'airdrop'), or in the event a previously supported Virtual Asset is no longer supported (e.g. as a result of a 'fork', or other change that would affect the VASP's ability to support the Virtual Asset), which shall include, but not be limited to obligations for the VASP to—
 - i. assess the impact of such change as soon as possible upon becoming aware of the nature and impact of such change; and
 - ii. communicate clearly with all affected clients throughout the process; and
 - c. address risk of loss which may result from a failure of the services provided by the VASP, including any Custody Services (if provided), and outline all measures in place to mitigate risk of loss where appropriate.
3. VASPs may provide the information required under Rule II.B.2 of this Market Conduct Rulebook by directing clients to where such information is contained in any published policies or procedures, provided that—
 - a. such policies or procedures comply with Rule II.A.4 of this Market Conduct Rulebook; and
 - b. all links or other references to such policies or procedures are maintained and accurate at all times.

Part III – Complaints Handling

A. Complaints Handling Requirements

1. Complaints handling. VASPs shall investigate all complaints promptly and resolve complaints as soon as practicable within a reasonable period of time, in accordance with the following requirements—
 - a. VASPs shall acknowledge all complaints within one (1) week of a complaint being made; and
 - b. VASPs shall resolve all complaints within four (4) weeks of the complaint being made, except in extraordinary circumstances, in which case VASPs must—
 - i. provide the client an update on the status of the complaint, and explain the extraordinary circumstances delaying its resolution, within four (4) weeks of the complaint being made; and
 - ii. resolve the complaint no later than eight (8) weeks from when the complaint was made.
2. VASPs shall make available to their clients an easy-to-use template form for filing complaints and provide accessible means, along with clear instructions, on where such complaints can be submitted, however shall not limit customers to only submitting complaints through one channel or in one form in order to be recognised as a complaint.
3. Where the provision of services relating to VA Activities involve any third-party Entities, VASPs shall establish procedures to facilitate the handling of such complaints between their clients and such third-party Entities. VASPs shall remain responsible for the resolution of such complaints.
4. VASPs shall not impose any fees or charges for the submission or handling of any complaints.
5. VASPs shall keep a record of—
 - a. all complaints received from their clients;
 - b. all measures they have taken in response to complaints; and
 - c. the resolution of all complaints.

B. Complaints Handling Procedures

1. VASPs shall establish and maintain effective procedures for the prompt, fair and consistent handling of complaints received from their clients in accordance with Rule III.A of this Market Conduct Rulebook. Such procedures shall be disclosed on their website in a clear and easy-to-understand manner.
2. Such procedures must establish when a VASP will consider a complaint to have been made and the mediums and channels through which it will monitor and recognise complaints.
3. When establishing and maintaining such procedures, VASPs must take reasonable steps to ensure that in handling complaints they identify and remedy any recurring or systemic problems, including but not limited to—
 - a. analysing the causes of complaints so as to identify common root causes of complaints;
 - b. considering whether such root causes may also affect other processes, services (including but not limited to VA Activities) or products, including those not directly complained of; and
 - c. correcting such root causes.

Part IV – Investor Classifications

A. Investor Classifications

1. General provision. VASPs shall only carry out a VA Activity, or attempt to carry out a VA Activity, in relation to the classifications of investors permitted by VARA, subject at all times to all restrictions imposed by VARA in any of the following—
 - a. Regulations, Rules or Directives as amended from time to time;
 - b. the VASP's Licence and applicable licensing conditions; and
 - c. further conditions imposed by VARA from time to time.
2. Retail Investor. A Retail Investor means an Entity that is not an Institutional Investor or a Qualified Investor.
3. Qualified Investor. A Qualified Investor means—
 - a. an individual that has relevant knowledge in respect of Virtual Assets, or complex structured products, for the nature of the VA Activities to be provided to the individual (the manner of demonstration of which, shall be defined by the VASP prior to offering any products or services and shall be demonstrated to VARA on request) and such individual—
 - i. maintains net assets (comprising fiat currency, financial instruments, Virtual Assets and/or equity in tangible real estate assets, or any combination thereof) of at least AED 3,500,000 in equivalent value, supported by documentary proof of funds (e.g. account statements) that illustrate the relevant assets have remained, and will remain, liquid for a reasonable period of time and which shall be checked periodically, provided that—
 1. the following assets shall be excluded from the calculation from an individual's net assets—
 - i. the value of property that is the individual's primary residence, including any equity held by the individual net of any obligation against that residence;
 - ii. any rights of the individual under a qualifying contract of insurance; and
 - iii. any benefits (in the form of pensions or otherwise), which are payable on the termination of the individual's service, or on death or retirement, and to which the individual or the individual's dependents are, or may be, entitled; and
 2. for the calculation of net assets, only 50% of the market value of Virtual Assets belonging to the individual may be included; or
 - ii. has an annual income of AED 700,000 or more; or
 - b. a legal entity validly incorporated in the jurisdiction in which it is located—
 - i. maintaining net assets (comprising fiat currency, financial instruments, Virtual Assets and/or equity in tangible real estate assets, or any combination thereof) of at least AED 3,500,000 in equivalent value supported by documentary proof of funds (e.g. account statements) that illustrate the relevant assets have remained, and will remain, liquid for a reasonable period of time and which shall be checked periodically, provided

that, for the calculation of net assets, only 50% of the market value of Virtual Assets belonging to the legal entity may be included; and

- ii. whose directors have relevant knowledge in respect of Virtual Assets for the nature of the VA Activities to be provided to the legal entity, the manner of demonstration of which shall be defined by the VASP prior to offering any products or services and shall be demonstrated to VARA on request.

4. Institutional Investor. An Institutional Investor means—

- a. any Entity regulated by a competent financial services regulator in the jurisdiction in which it is located (including but not limited to the CBUAE, the UAE Securities and Commodities Authority, the Dubai Financial Services Authority and the Financial Services Regulatory Authority of the Abu Dhabi Global Market);
- b. any VASP;
- c. any government with relevant knowledge in respect of Virtual Assets for the nature of the VA Activities to be provided, the manner of demonstration of which shall be defined by the VASP prior to offering any products or services and shall be demonstrated to VARA on request;
- d. any institution which performs the functions of a central bank; or
- e. any multilateral agency with relevant knowledge in respect of Virtual Assets for the nature of the VA Activities to be provided, the manner of demonstration of which shall be defined by the VASP prior to offering any products or services and shall be demonstrated to VARA on request.

Part V – Public Disclosures

VASPs shall ensure the information listed in this Part V of the Market Conduct Rulebook is provided in an easily accessible location on their website in a machine-readable format and is kept accurate and up-to-date at all times.

A. Licence Details and Authorised VA Activities

1. VASPs shall publish the Licence number issued to them by VARA.
2. VASPs shall publish all VA Activities they are Licensed by VARA to carry out in the Emirate (including any restrictions stated by VARA as a condition of their Licence) and the validity period of such Licences.
3. VASPs shall publish the names of all Responsible Individuals.

B. Risk Disclosure Statement

1. VASPs shall publish a detailed description of all material risks associated with Virtual Assets, including but not limited to a specific statement that Virtual Assets—
 - a. may lose their value in part or in full and are subject to extreme volatility at times;
 - b. may not always be transferable and some transfers may be irreversible;
 - c. may not be liquid;
 - d. some transactions are not private and may be recorded on public DLTs; and

- e. may be subject to fraud, manipulation, theft, including through hacks and other targeted schemes and may not benefit from legal protections.

Part VI – Market Transparency

A. Insider Lists

1. VASPs must maintain complete and up-to-date lists of all Entities, including their Board, Staff, Group, advisors, accountants or other third-party agents and service providers, and those of their Group, that have or may have access to Inside Information in the course of the VASP's business or carrying out their respective roles for the VASP ("Insider List"). VASPs shall update Insider Lists accordingly while such information remains Inside Information.
2. VASPs shall retain the Insider List for a period of at least eight (8) years after it is drawn up or updated and shall provide VARA with any Insider List upon request.
3. The Insider List shall include at least—
 - a. the identity of any Entity having access to Inside Information;
 - b. the reason for including that Entity in the Insider List;
 - c. the date and time at which that Entity obtained access to Inside Information; and
 - d. the date on which the Insider List was drawn up.
4. VASPs shall update all Insider Lists promptly, including the date of the update, where—
 - a. there is a change in the reason for including an Entity already on the Insider List;
 - b. there is a new Entity who has access to Inside Information and needs, therefore, to be added to the Insider List; and
 - c. an Entity ceases to have access to Inside Information.Each update shall specify the date and time when the change triggering the update occurred.
5. VASPs shall take all reasonable steps to ensure that any Entity on the Insider List acknowledges in writing the legal and regulatory duties entailed and is aware of the sanctions applicable to Insider Dealing and unlawful disclosure of Inside Information.

B. Board and Staff Positions

1. In addition to applicable requirements in the Company Rulebook, VASPs shall, for the purposes of promoting fair and transparent markets, preventing conflicts of interest and ensuring compliance with all relevant Regulations, Rules and Directives, implement policies to govern and monitor the transactions and positions of their Board members and Staff. Such policies shall, as a minimum, specify—
 - a. any Virtual Assets which Board members and Staff cannot transact or have a position, or any other economic interests, in;
 - b. any legal entities of which Board members and Staff cannot have any shareholding or hold a directorship; and
 - c. the forms in which Board members and Staff shall—
 - i. obtain prior approvals under Rule VI.B.2 of this Market Conduct Rulebook; and

- ii. provide notifications under Rule VI.B.3 of this Market Conduct Rulebook.

2. All Board members and Staff shall obtain written approval from the VASP prior to taking any of the following actions which is reasonably likely to cause actual or potential conflicts of interest—

- a. opening, modifying or closing any Virtual Asset positions held directly or indirectly on their own account;
- b. increasing or decreasing their shareholding (held directly or indirectly on their own account) in a legal entity other than the VASP;
- c. taking up a directorship in a legal entity other than the VASP; or
- d. all additional actions stated by the VASP in the policy established under Rule VI.B.1 of this Market Conduct Rulebook.

3. VASPs shall, at least every six (6) months, require Board members and Staff to notify them of—

- a. in relation to all Virtual Asset positions held directly or indirectly on their own account—
 - i. a description and the identifier of each Virtual Asset and/or related investments;
 - ii. the size of positions for each Virtual Asset and/or related investments;
 - iii. the nature of the transaction(s); and
 - iv. transaction history relevant to positions held.
- b. in relation to their shareholding, held directly or indirectly on their own account, or director roles in any legal entities other than the VASP—
 - i. the full name and place of organisation of the legal entity;
 - ii. the purpose of such shareholding and directorship;
 - iii. the shareholding percentage (if applicable); and
 - iv. full details of any renumeration for such director roles.

4. If a VASP has any information or reason to believe any Board member or Staff is likely to cause, or has caused, an actual or potential conflict of interest, it must take all necessary actions to ensure such conflict of interest is removed, including but not limited to—

- a. procuring the relevant Board member or Staff to divest the relevant Virtual Asset positions or shareholding;
- b. resign from the board of the other legal entity; or
- c. any other action required to remove the conflict of interest, either with respect to the other Entity or the VASP.

5. VASPs shall notify all Board members and Staff of their obligations under Rule VI.B of this Market Conduct Rulebook in writing prior to the start of their employment by the VASP.

Part VII – Trading Own Account

A. General Prohibition

1. VASPs are prohibited from actively investing their own, or their Group's, portfolio of Virtual Assets or any other assets.
2. The general prohibition in Rule VII.A.1 of this Market Conduct Rulebook above does not prevent VASPs from entering into transactions in Virtual Assets or any other assets for the purpose of prudent management of Net Liquid Assets required to be held by the VASP, or prudent management of the VASP's treasury and/or balance sheet, provided that, VASPs must maintain full records of all transactions, and such records must be held for a minimum period of eight (8) years.
3. VARA shall have sole and absolute discretion in determining whether any transactions in Virtual Assets, or any other assets, made by a VASP constitute actively investing with their own portfolio of Virtual Assets or any other assets. In making such determination VARA will take into account the following—
 - a. frequency of transactions;
 - b. the Virtual Assets or other assets involved in the transactions;
 - c. volume of transactions;
 - d. nature of transactions including duration; and
 - e. nature of any profits generated by such transactions and significance in relation to the financial condition of the VASP.

B. Group Entities

1. All Entities in the Emirate, including those which are in the same Group as a VASP, must comply with Regulation IV.A.7 (if applicable).
2. Irrespective of the applicability of Rule VII.B.1 of this Market Conduct Rulebook, VASPs must comply with the reporting requirements set out in the Compliance and Risk Management Rulebook in respect of all Entities in their Group that actively invests their own, or the Group's, portfolio of Virtual Assets or any other assets.

Part VIII – VA Standards

A. Requirement to have VA Standards

1. VASPs shall establish standards for the Virtual Assets it provides VA Activities in relation to ("VA Standards").
2. VASPs shall take all reasonable steps including, but not limited to, conducting relevant due diligence to ensure all Virtual Assets meet its VA Standards prior to, and at all times during, the VASP providing any VA Activities in relation to such Virtual Assets.
3. VASPs shall disclose their VA Standards on their website.
4. VA Standards shall, to the extent relevant to the VA Activity, include but not be limited to the following considerations in respect of all Virtual Assets—
 - a. its market capitalisation, fully diluted value and liquidity, and whether such metrics have trended downwards over time;
 - b. its design, features and use cases, whether or not intended by the Issuer or relevant developers;
 - c. whether there are features which may materially affect a VASP's compliance with applicable laws, Regulations, Rules or Directives, including but not limited to those relating to

- AML/CFT, sanctions, securities, intellectual property;
- d. regulatory treatment by VARA and other appropriate authorities (including those outside of the Emirate), in particular whether the issuance of the Virtual Asset has received any regulatory approvals;
- e. whether a Virtual Asset is prohibited by VARA or any other appropriate authorities (both inside or outside the UAE) in jurisdictions in which the VASP will provide VA Activities, or equivalent activities, in relation to such Virtual Asset;
- f. the security and immutability of the underlying DLT protocol;
- g. its future development (e.g. 'roadmap') as communicated by the Issuer and/or relevant developers;
- h. whether it may be susceptible to price manipulation for any reason and relevant mitigations that will be implemented by the VASP;
- i. whether potential or actual conflicts of interest may arise should a VASP provide any VA Activities in relation to the Virtual Asset and relevant mitigations;
- j. the background of its Issuer including, but not limited to, relevant experience in the Virtual Asset sector and whether it has been subject to any investigations or claims in relation to fraud or deceit;
- k. if the Virtual Asset represents rights to any other assets, the enforceability of such rights;
- l. sufficient assets are available to satisfy any obligation with respect to any VA Activities;
- m. VASPs shall ensure that Virtual Asset terms and conditions reflect, to the extent possible, the operation of any existing underlying physical market and avoid adverse impacts to such market (if applicable); and
- n. VASPs should review Virtual Asset terms and conditions on a periodic basis for appropriate correlation with any physical market to ensure such terms and conditions conform to standards and practices in that physical market (if applicable).

B. Implementation and Control

1. VASPs shall regularly, and on an ongoing basis, assess relevant information to ensure that a Virtual Asset that it provides VA Activities in relation to continues to meet its VA Standards.
2. VASPs must maintain all records relevant to such assessments for eight (8) years and provide such records for VARA's inspection upon request.
3. VASPs shall set conditions under which VA Activities in relation to a Virtual Asset may be suspended, including where a Virtual Asset no longer meets its VA Standards. VASPs shall have and implement all necessary operational procedures and controls in the event such conditions are met.
4. VASPs shall notify VARA as soon as possible after becoming aware that a Virtual Asset no longer meets its VA Standards and shall take such steps as VARA may direct to minimise any adverse impact on clients arising as a result.
5. VARA shall have the right to require the suspension of a VA Activity in respect of any Virtual Asset upon reasonable grounds it deems appropriate.

Schedule 1 – Definitions

Term	Definition
“AML/CFT”	has the meaning ascribed to it in the Regulations.
“Board”	has the meaning ascribed to it in the Company Rulebook.

“CBUAE”	means the Central Bank of the United Arab Emirates.
“Client Agreements”	has the meaning ascribed to it in Rule <u>II.A.1</u> of this Market Conduct Rulebook.
“Client Money”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Client VAs”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Custody Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Directive”	has the meaning ascribed to it in the Regulations.
“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to the term ‘Distributed Ledger Technology’ in the Dubai VA Law.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Group”	has the meaning ascribed to it in the Company Rulebook.
“Inside Information”	has the meaning ascribed to it in the Regulations.
“Insider Dealing”	has the meaning ascribed to it in the Regulations.
“Insider List”	has the meaning ascribed to it in Rule <u>VI.A.1</u> of this Market Conduct Rulebook.
“Institutional Investor”	has the meaning ascribed to it in Rule <u>IV.A.4</u> of this Market Conduct Rulebook.
“Issuer”	has the meaning ascribed to it in the Regulations.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Market Conduct Rulebook”	means this Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Marketing Regulations”	means the <u>Regulations on the Marketing of Virtual Assets and Related Activities 2024</u> , issued by VARA and as may be amended or superseded from time to time.
“Net Liquid Assets”	has the meaning ascribed to it in the Company Rulebook.
“Qualified Investor”	has the meaning ascribed to it in Rule <u>IV.A.3</u> of this Market Conduct Rulebook.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Responsible Individuals”	has the meaning ascribed to it in the Company Rulebook.
“Retail Investor”	has the meaning ascribed to it in Rule <u>IV.A.2</u> of this Market Conduct Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Staff”	has the meaning ascribed to it in the Company Rulebook.

“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VA Standards”	has the meaning ascribed to it in Rule <u>VIII.A.1</u> of this Market Conduct Rulebook.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity Licensed by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.

VA Activity and Other Rulebooks

Advisory Services Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Advisory Services Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out Advisory Services in the Emirate.

This Advisory Services Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out Advisory Services must also comply with the following Rulebooks applicable to all VASPs—

1. Company Rulebook;
2. Compliance and Risk Management Rulebook;
3. Technology and Information Rulebook;
4. Market Conduct Rulebook; and
5. All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

For the avoidance of doubt, where a VASP is Licensed by VARA to carry out other VA Activities in the Emirate in addition to Advisory Services, it must comply with all Rulebooks which apply to those other VA Activities. Unless otherwise stated, the Rules in VA Activity specific Rulebooks apply cumulatively for each VA Activity a VASP carries out.

Capitalised terms in this Advisory Services Rulebook have the meanings ascribed to them in the Regulations or as otherwise provided in Schedule 1.

Part I – Policies, Procedures and Public Disclosures

A. Policies and Procedures

1. In addition to all other requirements in the Regulations and Rulebooks, VASPs providing Advisory Services shall establish, implement and enforce appropriate written internal policies and procedures relating to the following—
 - a. how they ensure the independent basis of their advice;
 - b. how they ensure all Staff providing advice are sufficiently competent in accordance with Rule II.B.1 of this Advisory Services Rulebook; and
 - c. such other policies and procedures as VARA may require from time to time.
2. VASPs providing Advisory Services shall assess and, in any case, at least yearly review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.

B. Public Disclosures

1. VASPs providing Advisory Services shall publish on their website in a prominent place or make available by other publicly accessible means—
 - a. a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed;
 - b. their policies and procedures relating to data privacy, whistleblowing and handling of client complaints;
 - c. a statement of whether the VASP refers or introduces clients to other Entities including, but not limited to, other VASPs, and if so, a description of the terms of such arrangements, and the monetary or non-monetary benefits received by the VASP, including by way of reciprocation for any service or business;
 - d. a statement of whether the VASP has accounts, funds or Virtual Assets maintained by a third party and if so, provide the identity of that third party; and
 - e. such other information as VARA may require from time to time.
2. Other disclosable matters. To the extent permissible under applicable laws, VASPs providing Advisory Services shall publish on their website or by other publicly accessible means—
 - a. details of any past convictions or prosecutions of any member(s) of their Senior Management or Board, whether before the courts of the UAE or the courts of another jurisdiction; and
 - b. any such other information relating to their business or activities as VARA may reasonably require.
3. The disclosure requirements set out in this Rule I.B of the Advisory Services Rulebook are in addition to all disclosures required under the Market Conduct Rulebook and to all notifications to VARA required under the Compliance and Risk Management Rulebook.

Part II – Advisory Services Rules

A. Client Suitability

1. VASPs providing Advisory Services shall establish procedures to ensure that their clients understand the risks associated with investing in Virtual Assets and are financially able to satisfy any obligation which may arise from them acting upon advice provided by the VASP.
2. VASPs providing Advisory Services shall provide all advice regarding Virtual Assets in good faith and which is suitable for, and in the best interest of, each client. In order to ensure all advice complies with this Rule II.A.2 of the Advisory Services Rulebook, VASPs shall consider the following factors at a minimum in respect of each client—
 - a. knowledge and experience in investing in Virtual Assets;
 - b. investment objectives including, but not limited to, risk tolerance, time horizon and venues through which they can acquire Virtual Assets; and
 - c. financial circumstances including, but not limited to, their ability to bear sudden and significant losses or the proportion of their net worth which is invested in Virtual Assets.
3. VASPs providing Advisory Services shall collect all necessary information from clients for the purpose of assessing relevant factors in accordance with Rule II.A.2 of this Advisory Services Rulebook and take all reasonable steps to ensure such information is accurate and up-to-date. All such information shall be maintained for at least eight (8) years.
4. VASPs providing Advisory Services shall, in all advice provided to clients, specify how the advice is appropriate for a client by reference to the factors assessed by the VASP in accordance with Rule II.A.2 of this Advisory Services Rulebook.
5. VASPs providing Advisory Services must eliminate any conscious bias, and take all reasonable steps to eliminate any non-conscious bias, in order to prevent discrimination between clients on any grounds which is not in the best interests of a client receiving advice.

B. Staff Competency

1. In addition to all requirements in the Company Rulebook, VASPs providing Advisory Services shall ensure all of their Staff are knowledgeable, competent and suitably trained given the nature of their role. In assessing Staff competency, VASPs shall consider the following factors at a minimum in the context of the role of the Staff member concerned—
 - a. academic, professional and industry qualifications;
 - b. experience in the Virtual Assets sector, including but not limited to hands-on working experience acquired through their employment by Entities carrying out activities similar to VA Activities outside of the Emirate;
 - c. experience in conducting regulated investment-related activities similar to the provision of Advisory Services, whether or not related to Virtual Assets;
 - d. whether they have a good understanding of the VARA regulatory framework, including but not limited to the Regulations, Rules and Directives governing the provision of Advisory Services; and
 - e. industry standards as may be applicable to the Virtual Assets sector from time to time.

C. Verification of Information

1. VASPs providing Advisory Services shall only provide advice which does not contain statements, promises, forecasts or other types of information which they know or suspect to be misleading, false or deceptive or which they should have reasonably known to be misleading, false or deceptive at the time of making such statement, promise or forecast.

- Prior to making any statement, promise or forecast, VASPs providing Advisory Services shall verify factual information against appropriate and reliable source materials and shall use all reasonable endeavours to verify the continued accuracy of such information.

D. Methodology

- VASPs shall, in the course of providing Advisory Services, assess a broad range of Virtual Assets available to the client which must be sufficiently diverse such that the client's investment objectives are met.

Schedule 1 – Definitions

Term	Definition
“Advisory Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Advisory Services Rulebook”	means this Advisory Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Board”	has the meaning ascribed to it in the Company Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Directive”	has the meaning ascribed to it in the Regulations.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Staff”	has the meaning ascribed to it in the Company Rulebook.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.

“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity authorised by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.

Broker-Dealer Services Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Broker-Dealer Services Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out Broker-Dealer Services in the Emirate.

This Broker-Dealer Services Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out Broker-Dealer Services must also comply with the following Rulebooks applicable to all VASPs—

1. Company Rulebook;
2. Compliance and Risk Management Rulebook;
3. Technology and Information Rulebook;
4. Market Conduct Rulebook; and
5. All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

For the avoidance of doubt, where a VASP is Licensed by VARA to carry out other VA Activities in the Emirate in addition to Broker-Dealer Services, it must comply with all Rulebooks which apply to those other VA Activities. Unless otherwise stated, the Rules in VA Activity specific Rulebooks apply cumulatively for each VA Activity a VASP carries out.

Capitalised terms in this Broker-Dealer Services Rulebook have the meanings ascribed to them in the Regulations or as otherwise provided in Schedule 1.

Part I – Policies, Procedures and Public Disclosures

A. Policies and Procedures

1. In addition to all other requirements in the Regulations and Rulebooks, VASPs providing Broker-Dealer Services shall establish, implement and enforce appropriate written internal policies and procedures relating to the following—
 - a. the prohibition, detection, prevention and/or deterrence of Market Offences and any other abusive practices within their business or using their services including, but not limited to, relevant internal rules, compliance programmes, sanctioning policies and powers;
 - b. execution and routing of client orders;

- c. the ability of clients to have access to and withdraw their Virtual Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility; and
- d. such other policies and procedures as VARA may require from time to time.

2. VASPs providing Broker-Dealer Services shall assess and, in any case, at least yearly review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.]

B. Public Disclosures

1. VASPs providing Broker-Dealer Services shall publish on their website in a prominent place or make available by other publicly accessible means—
 - a. a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed;
 - b. their policies and procedures relating to data privacy, whistleblowing and handling of client complaints;
 - c. a summary containing the following information pertaining to each Virtual Asset offered by the VASP—
 - i. name and symbol;
 - ii. date of issuance;
 - iii. market capitalisation and fully diluted value;
 - iv. circulating supply, including as a percentage of maximum total supply (if applicable);
 - v. whether the Virtual Asset has been subject to an independent smart contract audit and the date of the most recent audit;
 - vi. highest and lowest price including when each occurred, stated as both an absolute amount and a percentage change from the current price; and
 - vii. largest reduction in price from high to low, stated as both an absolute amount and a percentage change, during any day, month and year and including when each occurred;
 - d. a description of how the VASP determines the prices of the Virtual Assets it quotes to clients;
 - e. a description of the VASP's routing practices, including if twenty percent (20%) or more of client orders are routed to any liquidity source and if so, the identity of such source(s);
 - f. a statement as to whether the VASP holds or maintains funds or Virtual Assets or provides clearing services for other VASPs providing Broker-Dealer Services and if so, include a description of those services;
 - g. a statement as to the VASP's arrangements for the protection of clients' ownership of assets held by the VASP;
 - h. a statement of whether the VASP refers or introduces clients to other Entities including, but not limited to, other VASPs and, if so, a description of the terms of such arrangements and the monetary or non-monetary benefits received by the VASP, including by way of reciprocation for any service or business; and
 - i. a statement of whether the VASP has accounts, funds or Virtual Assets maintained by a third party and if so, provide the identity of that third party.

2. Other disclosable matters. To the extent permissible under applicable laws, VASPs providing Broker-Dealer Services shall publish on their website or by other publicly accessible means—
 - a. details of any past convictions or prosecutions of any member(s) of their Senior Management or Board, whether before the courts of the UAE or the courts of another jurisdiction; and
 - b. any such other information relating to their business or activities as VARA may reasonably require.
3. The disclosure requirements set out in this Rule I.B of the Broker-Dealer Services Rulebook are in addition to all disclosures required under the Market Conduct Rulebook and to all notifications to VARA required under the Compliance and Risk Management Rulebook.

Part II – Trading and Execution Rules

A. Best Execution

1. VASPs must exercise reasonable diligence to Execute each client order to buy or sell one or more Virtual Assets that it receives so as to obtain the most favourable price for the client under the prevailing market conditions, provided that due consideration is also given to costs, speed, likelihood of Execution and settlement, size, nature or any other consideration relevant to the Execution of the order to ensure the best possible result for the client.
2. Rule II.A.1 of this Broker-Dealer Services Rulebook applies to the handling of all orders to buy or sell one or more Virtual Assets, except in the following two scenarios (provided that both sub-conditions thereunder are met in either scenario)—
 - a. the client making the order to buy or sell one or more Virtual Assets is another VASP that has already secured a VARA Licence, and that shall be the responsible Entity to its end client for the instruction (for the purposes of this Rule II.A.2.a only, “**VASP-A**”), and—
 - i. such VASP-A has specifically asked the VASP carrying out Broker-Dealer Services that is receiving the order (for the purposes of this Rule II.A.2.a only, “**VASP-B**”) to provide it with a quote to Execute at the discretion of VASP-B; and
 - ii. such VASP-B does not satisfy the order by dealing as principal; or
 - b. the client making the order to buy or sell one or more Virtual Assets is a Qualified Investor or an Institutional Investor, and—
 - i. the client has specifically asked the VASP carrying out Broker-Dealer Services to provide it with a quote to Execute, and has authorised the VASP to do so at the VASP's professional discretion; and
 - ii. the VASP carrying out Broker-Dealer Services does not satisfy such client order by dealing as principal with the client making the order.
3. VASPs shall have written controls in place to ensure that the best Execution standard in Rule II.A.1 of this Broker-Dealer Services Rulebook is met and that any conflicts of interest either between competing client orders or between client orders and the interests of the VASP are managed appropriately.
4. Among the factors that will be considered in determining whether a VASP has taken steps to obtain the best possible result for the purposes of Rule II.A.1 of this Broker-Dealer Services

Rulebook are—

- a. the characteristics of the Market for the Virtual Asset (e.g. price, spreads, volatility, relative liquidity, and pressure on communications);
- b. the size and type of transaction;
- c. the number of Markets or other sources of liquidity checked;
- d. accessibility of quotes to trade in the Virtual Asset(s) in question under the market conditions prevailing at the relevant time, noting that, even in the event that certain sources of liquidity are not available, VASPs are not relieved from taking reasonable steps and employing their market expertise in seeking to achieve the best Execution of client orders; and
- e. the terms and conditions of the order which result in the transaction, as communicated to the VASP.

5. Where a VASP Executes a client order off-Market by trading with another VASP or another third party, the burden of demonstrating compliance with the best Execution standard set out in Rule II.A.1 of this Broker-Dealer Services Rulebook shall remain with the VASP.
6. When Executing client orders, VASPs shall disclose to their clients, both prior to Execution and in the trade confirmation, the portion of the amount payable by the client that is retained by the VASP as fees or commission for the trade, except where a VASP provides another VASP, a Qualified Investor or an Institutional Investor with a quote to Execute at the VASP's discretion under Rule II.A.2 of this Broker-Dealer Services Rulebook.
7. VASPs shall not pay or receive any monetary or non-monetary benefit, including by way of reciprocation for any service or business, to any third party in respect of its Execution services provided to a client, except for necessary service fees required to Execute the client's order. In particular, VASPs shall not receive any remuneration, discount or non-monetary benefit for routing clients' orders to a particular trading venue or to another Entity. Any fees payable by or to another VASP or other third party shall be structured in such a way so as not to give rise to conflicts of interest in respect of the Execution of client orders.
8. For the avoidance of doubt, failure to maintain or adequately resource a department assigned to Execute clients' orders cannot be considered justification for not complying with the Execution requirements in this Part II of the Broker-Dealer Services Rulebook.
9. A VASP through which an order is channelled and that knowingly is a party to an arrangement whereby the initiating VASP has not fulfilled its obligations under this Part II of the Broker-Dealer Services Rulebook, will also be deemed to have violated this Part II.
10. If a VASP receives an unsolicited instruction from a client to route that client's order to a particular Market or counterparty for Execution, the VASP is not required to make a best Execution determination beyond the client's specific instruction, provided that the VASP processes the client's order promptly in accordance with its terms.
11. Where a client has directed that an order be routed to another specific VASP that is also Licensed by VARA, the receiving VASP to which the order was directed is required to meet the requirements in this Part II of the Broker-Dealer Services Rulebook with respect to its handling of the order.
12. Each VASP must document its compliance with its policies and procedures related to its selection of the best Market for a Virtual Asset, including how to Execute client orders where there is an absence of pricing information, an absence of drivers or valuation factors behind such prices, or multiple quotations.
13. No VASP can delegate to another Entity responsibility to provide best Execution to its client's orders. VASPs that route client orders to other Entities for Execution on an automated, non-discretionary basis, as well as VASPs that internalise client order flows, must review (at least quarterly) the quality of Execution received by their clients, with reference to how such Execution

quality compares with the Execution quality the VASP may have obtained from other Markets or sources of liquidity. In conducting each such reviews, VASPs must determine whether any material differences in Execution quality exist among the Virtual Assets trading and, if so, modify their routing arrangements or justify why they are not modifying their routing arrangements.

14. VASPs that route their order flows to another Entity that has agreed to handle that order flow as agent for the client can rely on that Entity's regular and rigorous review, as long as the rationale of the review is fully disclosed to the originating VASP.
15. VASPs shall develop, implement and maintain systems to ensure that their systems have the capacity and capabilities to Execute client orders received through such systems or such other means as may be agreed with clients from time to time.
16. VASPs must notify clients with whom they have an ongoing relationship of any material changes to their order Execution arrangements or their Execution policy.

B. Dealing as Principal

1. VASPs shall be permitted to deal as principal (including as riskless principal) for the purpose of satisfying client orders, placing of Virtual Assets and/or managing the VASP's inventory of Virtual Assets and other assets, subject to complying with the best Execution standard set out in Rule II.A.1 of this Broker-Dealer Services Rulebook above.
2. For the avoidance of doubt, it is prohibited for a VASP, when dealing as principal or otherwise, to use or otherwise deal in Client Money or Client VAs except as expressly permitted under Parts IV and V of the Compliance and Risk Management Rulebook.

C. Advisory Services

1. VASPs providing Broker-Dealer Services may carry out Advisory Services in the Emirate, provided that they shall—
 - a. continue to hold, and to comply with all requirements of, their Licence to carry out Broker-Dealer Services;
 - b. comply with all Capital and Prudential Requirements in the Company Rulebook that apply to Advisory Services in addition to those required for Broker-Dealer Services; and
 - c. comply with the Advisory Services Rulebook in respect of all Advisory Services.

Part III – Margin Trading Rules

A. Compliance with Margin Trading Rules

1. VASPs may only provide Margin Trading services if explicitly authorised to do so by VARA and such authorisation is expressly stipulated in their Licence.
2. VASPs that are authorised to provide Margin Trading services, must comply with this Part III of the Broker-Dealer Services Rulebook at all times when providing Margin Trading services.
3. VASPs must ensure that they have sufficient assets to provide Margin Trading services in order that they can fully satisfy client obligations, at all times.

B. VARA Approval and Powers

1. VARA may approve an application for the provision of Margin Trading services, provided that the VASP can demonstrate, to VARA's satisfaction, compliance with the following requirements—
 - a. the VASP has submitted for VARA's approval details of the terms and conditions upon which it proposes to offer Margin Trading services to clients, including a copy of the template Margin Trading Agreement to be used by the VASP, together with information relating to the VASP's financial condition and compliance with all Capital and Prudential Requirements applicable to the VASP;
 - b. the VASP has established, and is able to demonstrate to VARA upon request, appropriate policies and procedures as well as systems and controls with regards to Margin Trading services, which shall include but not be limited to—
 - i. the Margin which may be called, the applicable Margin rates and the method of calculating the Margin;
 - ii. the acceptable methods of Margin payment and forms of collateral;
 - iii. the circumstances under which a client or counterparty may be required to provide Margin and additional Margin, and the consequences of a failure to meet a Margin call, including the actions which the VASP may be entitled to take; and
 - iv. applicable escalation procedures where a client or counterparty fails to meet Margin calls; and
 - c. the VASP ensures, and is able to demonstrate to VARA upon request, that Virtual Assets collected as collateral for Initial Margin and Maintenance Margin purposes are liquid and can be liquidated within a reasonable timeframe.
2. VARA may request to inspect the Margin Trading system of the VASP used to calculate clients' Margin Trading positions and Margin, and prior to granting approval, request any other clarification, information or documents it deems necessary.
3. Notwithstanding a VASP having approval from VARA for the provision of Margin Trading, VARA shall have the power to instruct VASPs to take any of the following actions, in its sole and absolute discretion from time to time, and VASPs must comply with such instructions—
 - a. suspend Margin Trading services for specified Virtual Assets or clients;
 - b. close existing client positions; and
 - c. increase Initial Margin and/or Maintenance Margin requirements.

C. Margin Trading Obligations

1. Without prejudice to any other obligations, VASPs providing Margin Trading services shall—
 - a. obtain information from each client prior to opening a Margin Trading Account to determine whether the Margin Trading service is suitable for a particular client, including but not limited to such information on the client's financial position (including financial solvency), investment objectives, risk appetite, knowledge and experience in trading in Virtual Asset markets as may be relevant and practical;
 - b. ensure that each client's Margin Trading Account is segregated from all other trading accounts;
 - c. only use all Virtual Assets and/or cash balance in the Margin Trading Account as collateral for Margin Trading in accordance with the terms of the Margin Trading Agreement;

- d. not to utilise the funds of any client to provide the facilities of Margin Trading to another client, even if the client's consent has been obtained by the VASP;
- e. ensure that each client has deposited the Initial Margin in the Margin Trading Account, in accordance with the agreed value, prior to the purchase of any Virtual Assets financed on Margin;
- f. ensure that, if a client has more than one (1) Margin Trading Account with the VASP, that all risk limits are monitored and maintained at the client level;
- g. provide each client with a written statement of account at least monthly showing the trading movement of the Virtual Assets financed on Margin and the percentage of their ownership in the Margin Trading Account relative to any Virtual Assets, cash or other assets held as Maintenance Margin;
- h. monitor on an ongoing basis the Margin Trading Account of each client and provide at least one (1) early warning notification to a client that the percentage of the client's ownership in that account has fallen to a specified percentage and is at risk of falling below the required level of Maintenance Margin specified in the Margin Trading Agreement. The specified percentage at which such early warning notification must be given may be determined by the VASP acting in the best interests of its clients. Such notification must include a full re-statement of the risks required to be stated in the Margin Trading Agreement in Rule III.E.1.d of this Broker-Dealer Services Rulebook below;
- i. in addition to Rule III.C.1.h of this Broker-Dealer Services Rulebook above, monitor on an ongoing basis the Margin Trading Account of each client and notify the client promptly when the percentage of the client's ownership in that account falls below the required level of Maintenance Margin specified in the Margin Trading Agreement, so that they can cover the shortfall in the account, subject to Rule III.C.1.j of this Broker-Dealer Services Rulebook below;
- j. in the event that the client is not themselves able to remedy the shortfall within a reasonable timeframe, sell all or some of the Virtual Assets available in the Margin Trading Account to the extent required to restore the client's percentage of ownership to the Maintenance Margin (or such higher level as may be set out in the Margin Trading Agreement) as per the market value of such Virtual Assets on the date of sale;
- k. obtain the prior approval of VARA on any subsequent amendment to the Margin Trading system described in Rule III.B.2 of this Broker-Dealer Services Rulebook above, and provide a technical report confirming that the amended system is able to fulfil the requirements of the Margin Trading service on an ongoing basis, including during times of high volatility; and
- l. ensure that orderly records are kept for the Margin Trading services undertaken by them for a period of at least eight (8) years.

D. Prudential Requirements, Initial Margin and Maintenance Margin

1. VASPs authorised by VARA to provide Margin Trading services shall—
 - a. ensure that the aggregate funds allocated for Margin Trading services by the VASP are included in the VASP's calculation of its Operational Exposure; and
 - b. ensure that the amount of credit extended to a single client for Margin Trading does not exceed one tenth of the total funds directly or indirectly attributable to Margin Trading by the VASP in its Operational Exposure, in accordance with Rule III.D.1.a of this Broker-Dealer Services Rulebook above.

2. VASPs may only accept the following types of collateral in a Margin Trading Account—
 - a. the Virtual Asset financed on Margin in that account;
 - b. fiat currency; and
 - c. Virtual Asset referencing USD or AED, as approved by VARA.
3. Notwithstanding Rule III.D.2 of this Broker-Dealer Services Rulebook, VASPs may accept the following types of collateral in a Margin Trading Account in the following circumstances—
 - a. other Virtual Assets where there is a continuing fall in the market value of the Virtual Asset financed on Margin; and
 - b. other Virtual Assets where trading in the Virtual Asset financed on Margin is suspended or discontinued for more than seven (7) Working Days or such other period prescribed by VARA.

E. Margin Trading Agreement

1. The Margin Trading Agreement must include the following information—
 - a. an explanation of the VASP's responsibilities and the respective obligations of the VASP and the client including, but not limited to, termination rights, the effect of termination, applicable dispute resolution mechanisms and the VASP's obligation to provide an early warning notification under Rule III.C.1.h of this Broker-Dealer Services Rulebook including when such notifications will be provided;
 - b. whether the client has the right to withdraw cash from the Margin Trading Account, transfer amounts from the Margin Trading Account to the other account, or use such funds for new Margin financing if these amounts are higher than the Maintenance Margin;
 - c. how all financing is calculated, including but not limited to how and when it is paid or payable, the applicable rate, or in the case of a variable rate, how it is calculated and how it may vary and how such variations will be communicated by the VASP to the client;
 - d. an explanation of the following risks the client may be exposed to when undertaking Margin Trading, including but not limited to—
 - i. the risk that the client may lose all or part of the funds deposited in the Margin Trading Account;
 - ii. the fact that the VASP may request that the client add Virtual Assets and/or funds in the Margin Trading Account if the Maintenance Margin falls below the prescribed levels or if the VASP increases Maintenance Margin requirements;
 - iii. the right of the VASP to sell all or part of the Virtual Assets in the Margin Trading Account if the Maintenance Margin falls below the percentage specified in the Margin Trading Agreement; and
 - iv. when and how the VASP may sell all or part of the Virtual Assets in the Margin Trading Account;
 - e. express consent from the client that they understand, acknowledge and accept each of the risks listed in Rule III.E.1.d of this Broker-Dealer Services Rulebook above;
 - f. the applicable levels of Initial Margin and Maintenance Margin and circumstances in which Initial Margin and Maintenance Margin can be amended by the VASP;

- g. a breakdown of the commissions, charges and fees charged by the VASP relating to Margin Trading and when they are payable;
- h. a confirmation of the client's right to pay the cash balance of the price of the remaining Virtual Assets in the Margin Trading Account at any time; and
- i. the fact that in certain situations the position of the client may be liquidated, and that following such liquidation the client may be required to make an additional payment to the VASP.

2. VARA may require any amendments to the Margin Trading Agreement or other forms relating to Margin Trading conducted by a VASP as it deems appropriate.

Part IV - Licensed Distribution Services Rules

A. Compliance with Licensed Distribution Services Rules

- 1. VASPs that have a Licence from VARA to carry out Broker-Dealer Services must comply with this Part IV of the Broker-Dealer Services Rulebook, at all times, when providing Licensed Distribution Services.
- 2. All Rules in this Part IV of the Broker-Dealer Services Rulebook apply in addition to all other requirements in the Regulations and Rulebooks, as may be in force from time to time. In the event of a conflict, the Rules in this Part IV of the Broker-Dealer Services Rulebook shall have precedence in respect of Licensed Distribution Services only.
- 3. VARA shall, in its sole and absolute discretion, have the power to instruct a VASP to take any of the following actions, from time to time, and the VASP shall comply with such instructions—
 - a. suspend Licensed Distribution Services for specified Virtual Assets, Issuers or clients; or
 - b. cease Licensed Distribution Services for specified Virtual Assets, Issuers or clients.

B. Licensed Distribution Services Obligations and Responsibility

- 1. Responsibility. VASPs providing Licensed Distribution Services must ensure beyond all reasonable doubt, the quality of all Issuers and Virtual Assets for which it provides Licensed Distribution Services.
- 2. Quality, as referred to in Rule IV.B.1, shall include, but not be limited to all factors relevant to assurance of the following—
 - a. consumer protection and preventing harms arising from misinformation and/or abusive practices, ensuring consumers are appropriately informed and have provided consent prior to engaging with risk;
 - b. full FATF and financial sanctions compliance, and zero tolerance of money laundering, financing of terrorism or destructive proliferation activities;
 - c. zero tolerance of any fraud, theft or other illicit or criminal activity;
 - d. fair, orderly and transparent markets, including full compliance with VARA's Market Offences as defined in the Regulations;
 - e. technical and/or cyber security exposures associated with the Virtual Asset and/or with the act of issuance or throughout the process of issuing or transferring the Virtual Asset;
 - f. compliance with all applicable laws and regulations; and

- g. compliance with the VA Issuance Rulebook.

3. Due diligence and assessment of Virtual Assets. VASPs providing Licensed Distribution Services shall carry out comprehensive due diligence on each Virtual Asset for which it provides Licensed Distribution Services, in order to ensure the quality of such Virtual Asset, in compliance with Rule IV.B.1. Such due diligence shall include, but not be limited to, the following—

- a. that the Virtual Asset complies with the VASP's VA Standards;
- b. that the Whitepaper complies with Part III.B of the VA Issuance Rulebook;
- c. that the Risk Disclosure Statement complies with Part III.C of the VA Issuance Rulebook;
- d. compliance with Part IV of the Market Conduct Rulebook in regard to investor classifications; and
- e. all smart contracts used for the purposes of the Virtual Asset have undergone comprehensive audits of their effectiveness, enforceability and robustness and that all findings from such audits have been satisfactorily remediated.

4. Due diligence and assessment of Issuer. VASPs providing Licensed Distribution Services shall carry out comprehensive due diligence on all Issuers to whom they provide Licensed Distribution Services to ensure the quality of the Issuer, in compliance with Rule IV.B.1. Such due diligence shall include, but not be limited to, the following—

- a. that the Issuer complies with Part II of the VA Issuance Rulebook; and
- b. the VASP meets its requirements under Part III.E – Client due diligence of the Compliance and Risk Management Rulebook.

5. Disclaimer. VASPs must ensure that all documentation, including all Whitepapers, relating to Virtual Assets for which it provides Licensed Distribution Services contains the following disclaimer:

- a. '*VARA has not made any representation and does not provide any warranties regarding any Issuer or Virtual Asset including, but not limited to, their fitness for purpose, suitability or regulatory status in any jurisdiction other than the Emirate of Dubai, UAE.*'

C. Relationship with the Issuer

- 1. Written agreements. VASPs must have written Client Agreements with all Issuers to whom they provide Licensed Distribution Services in compliance with Part II of the Market Conduct Rulebook.
- 2. Conflicts of interest. In addition to all existing requirements in Part II.C of the Company Rulebook, VASPs providing Licensed Distribution Services must have, and implement written controls to prevent, monitor, manage and disclose any conflicts of interest when providing Licensed Distribution Services. Such controls must address, but not be limited to—
 - a. the pricing of the initial placement or distribution of all Virtual Assets; and
 - b. conditions on which the VASP may receive an allocation of, or purchase, the Virtual Assets including for the purposes of dealing as principal, making a market, or by way of renumeration for the VASPs services.

D. Submissions to VARA

1. VASPs providing Licensed Distribution Services must submit the following documents (in the form prescribed by VARA on its website from time to time) in respect of all Virtual Assets for which it provides Licensed Distribution Services—
 - a. the Whitepaper;
 - b. the Risk Disclosure Statement;
 - c. a declaration, signed by the VASP, of its compliance with Rule IV.B.1 of this Broker-Dealer Services Rulebook; and
 - d. reports on the due diligence carried out under Rules IV.B.3 and IV.B.4 of this Broker-Dealer Services Rulebook.
2. Starting from the first Working Day after the submissions required under Rule IV.D of this Broker-Dealer Services Rulebook are made, a submission period of fifteen (15) Working Days shall commence (“**Submission Period**”).
3. No Virtual Asset may be distributed or placed prior to completion of the Submission Period.
4. If a VASP has not received any comment or objection from VARA during the Submission Period , the VASP may distribute or place the Virtual Assets for which such submissions were made.
5. In addition, and without prejudice, to all of VARA's existing powers of suspension and/or other enforcement actions contained in the Regulations or Rulebooks, VARA may comment on or object to the distribution or placement of any Virtual Asset during the Submission Period.
6. Upon receipt of such comment or objection, the VASP providing Licensed Distribution Services must not distribute or place the Virtual Assets for which such submissions were made until all such comments have been addressed and/or objections remedied, to VARA's satisfaction.
7. For the avoidance of doubt, in no event shall VARA be deemed to have approved any Virtual Asset or Licensed Distribution Services by virtue of a VASP's compliance with Rules IV.D.1 and IV.D.2 of this Broker-Dealer Services Rulebook, including, but not limited to, in the event of the expiry of the Submission Period without comment or objection from VARA.

E. Ongoing Obligations, Monitoring and Notification

1. Monitoring. VASPs providing Licensed Distribution Services must ensure that all due diligence carried out under Rules IV.B.3 and IV.B.4 remains up-to-date and accurate at all times during which the VASP is providing Licensed Distribution Services to the Issuer and/or in respect of the relevant Virtual Asset.
2. VASPs must immediately suspend and/or cease any Licensed Distribution Services in relation to any Virtual Asset if the VASP knows, or has reason to suspect, the Virtual Asset no longer complies with Rule IV.B of this Broker-Dealer Services Rulebook.
3. In the event of any material change to an Issuer or a Virtual Asset, including but not limited to any factors listed in Rule IV.B.2, for which a VASP provides Licensed Distribution Services, the VASP must—
 - a. immediately carry out the due diligence required under Rules IV.B.3 and IV.B.4 of this Broker-Dealer Services Rulebook including in respect of all changes since due diligence was last completed;
 - b. suspend all Licensed Distribution Services immediately upon becoming aware of the Issuer or Virtual Asset not satisfying Rule IV.B; and

c. comply with Rule IV.D including in respect of all changes since the last submission to VARA was made in accordance with Rule IV.D of this Broker-Dealer Services Rulebook.

Schedule 1 – Definitions

Term	Definition
“Advisory Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Advisory Services Rulebook”	means the Advisory Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Board”	has the meaning ascribed to it in the Company Rulebook.
“Broker-Dealer Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Broker-Dealer Services Rulebook”	means this Broker-Dealer Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Capital and Prudential Requirements”	has the meaning ascribed to it in the Company Rulebook.
“Client Agreements”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Client Money”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Client VAs”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Execute” or “Execution”	means the exercise of a client order that results in a binding transaction.
“Initial Margin”	<p>means the minimum value of assets which must be deposited by the client in the Margin Trading Account, or otherwise available in the Margin Trading Account but not committed to an existing Margin Trading position, prior to the client opening any new Margin Trading position, which shall be calculated as follows—</p> <p>(a) for Retail Investors—</p> <ul style="list-style-type: none"> i. a minimum of twenty percent (20%) of the notional position value of the new Margin Trading position; or ii. such greater amount as VARA may require for a specific VASP, Virtual Asset or client, from time to time; and <p>(b) for Qualified Investors and Institutional Investors—</p> <ul style="list-style-type: none"> i. such amounts as determined by the VASP's policy; or

	<p>ii. such greater amount as VARA may require for a specific VASP, Virtual Asset or client, from time to time.</p>
"Institutional Investor"	has the meaning ascribed to it in the Market Conduct Rulebook.
"Issuer"	has the meaning ascribed to it in the Regulations.
"Licence"	has the meaning ascribed to it in the Regulations.
"Licensed"	means having a valid Licence.
"Licensed Distribution Services"	<p>means providing placement, distribution and/or other issuance related services to Issuers of Virtual Assets.</p> <p>For the purposes of this definition, "issuance related services" may include end-to-end solutions for the creation, placing, distribution and marketing conducted by a VASP for or on behalf of the Issuer as well as the actual sale or placement of any Virtual Assets, or any combination thereof.</p>
"Maintenance Margin"	means the value of assets which must be deposited by the client in the Margin Trading Account, or otherwise available in the Margin Trading Account but not committed to an existing Margin Trading position, to keep a Margin Trading position open.
"Margin"	means the Initial Margin and any Maintenance Margin provided by a client.
"Margin Trading"	means the financing made by a VASP of a proportion or multiple of the market value of the Virtual Assets financed on margin, and secured as collateral by the Virtual Assets available in the Margin Trading Account or any other collateral in the cases exclusively stated in these Rules.
"Margin Trading Account"	means a type of client account with the VASP, through which dealings in Virtual Assets financed on Margin are executed.
"Margin Trading Agreement"	means the agreement between the VASP and the client specifying the terms and conditions governing the relationship between them in relation to Margin Trading.
"Market"	<p>means a variety of different venues, including but not limited to, market centres that are trading a particular Virtual Asset*.</p> <p>*This expansive interpretation is meant to inform VASPs providing Broker-Dealer Services as to the breadth of the scope of venues that must be considered in the furtherance of their best Execution obligations and to promote fair competition among VASPs providing Broker-Dealer Services, Exchange Services, as well as any other venue that may emerge, by not mandating that certain trading venues have less relevance than others in the course of determining a VASP's best Execution obligations.</p>
"Market Conduct Rulebook"	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended VARA from time to time.
"Market Offences"	has the meaning ascribed to it in the Regulations.
"Operational Exposure"	has the meaning ascribed to it in the Company Rulebook.
"Qualified Investor"	has the meaning ascribed to it in the Market Conduct Rulebook.
"Regulations"	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.

“Retail Investor”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Risk Disclosure Statement”	has the meaning ascribed to it in the VA Issuance Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Submission Period”	has the meaning ascribed to it in Rule <u>IV.D.2</u> of this Broker-Dealer Services Rulebook.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended VARA from time to time.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VA Issuance Rulebook”	means the Virtual Asset Issuance Rulebook issued by VARA pursuant to the Regulations, as may be amended or supplemented by VARA from time to time.
“VA Standards”	has the meaning ascribed to it in the Market Conduct Rulebook.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity authorised by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.
“Whitepaper”	has the meaning ascribed to it in the VA Issuance Rulebook.
“Working Day”	has the meaning ascribed to it in the Regulations.

Custody Services Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Custody Services Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out Custody Services in the Emirate.

This Custody Services Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out Custody Services must also comply with the following Rulebooks applicable to all VASPs—

1. Company Rulebook;
2. Compliance and Risk Management Rulebook;
3. Technology and Information Rulebook;
4. Market Conduct Rulebook; and
5. All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

As stated in Rule III.B.5 of this Custody Services Rulebook, VASPs providing Custody Services must be an independent legal Entity – separate from any member of their Group that provides other VA Activities or linked services – except in respect of VA Transfer and Settlement Services.

For the avoidance of doubt, where a VASP is Licensed by VARA to carry out VA Transfer and Settlement Services in the Emirate, in addition to Custody Services, it must comply with the VA Transfer and Settlement Services Rulebook. Unless otherwise stated, the Rules in VA Activity specific Rulebooks apply cumulatively for each VA Activity a VASP carries out.

Capitalised terms in this Custody Services Rulebook have the meanings ascribed to them in the Regulations or as otherwise provided in Schedule 1.

Part I – Additional Board Requirements

A. Board Constitution

1. The Board of a VASP providing Custody Services shall consist of executive directors and non-executive directors, with a minimum of one (1) director qualifying as an independent director as set out below.
2. The Board of a VASP providing Custody Services shall convene at least on a quarterly basis.
3. VASPs providing Custody Services shall mandate the length of each term, and number of terms each Board member may serve on the Board.
4. A Board member is not regarded as an independent director of a VASP if—
 - a. they or any of their first-degree relatives are working or have worked as a member of the Senior Management, or held a role in the VASP's Group equivalent to Senior Management within the two (2) years preceding the date of their nomination to the Board;
 - b. they or any of their first-degree relatives have a direct or indirect interest in the contracts and projects concluded with the Group during the preceding two (2) years, provided that the aggregate value of such contracts and projects do not exceed the lower of (i) ten percent (10%) of the Paid-Up Capital of the VASP, or (ii) the amount of AED 5,000,000 or its equivalent in other foreign currency, unless such contracts and projects relate to the ordinary course of business of the VASP and do not contain any preferential conditions;
 - c. they are working or have worked for the Group during the two (2) years preceding the date of their appointment to the Board;
 - d. they work for, or are a partner of a company that performs consultancy services for the VASP or any members of its Group, or has performed such services during the preceding two (2) years;
 - e. they have any personal service contracts with the VASP or any members of its Group, or have had such contract during the preceding two (2) years, excluding any contract under which they are appointed as a non-executive director;
 - f. they are directly or indirectly linked to any Entity that receives substantial funding from the VASP's Group;
 - g. they or any of their first-degree relatives are a partner or an employee of the auditor of the VASP, or if, during the two (2) years preceding the date of their Board membership, were a partner or an employee of the auditor of the VASP;
 - h. the ownership held by them and their first-degree relatives reaches ten percent (10%) or more of the share capital of the VASP;
 - i. they have served more than seven (7) years as a Board member of the VASP; or

- j. they are the representative of an investor in the VASP holding ten percent (10%) or more of the share capital of the VASP.

B. Board Committees

1. The Board of a VASP providing Custody Services shall establish remuneration, nomination and audit committees, and may establish additional committees, to perform certain delegated functions on behalf of the Board. The Board may delegate specific authority, but not its responsibilities, to such committees, provided that it continuously monitors and oversees the work conducted by all committees.
2. Each committee created by the Board of a VASP providing Custody Services shall—
 - a. have a charter or other instrument that sets out its membership, mandate, scope, working procedures and means of accountability to the Board; and
 - b. report to the Board on findings and recommendations relating to the work entrusted by the Board to it regularly.
3. The Board and its committees shall keep minutes to record details of the matters discussed, recommendations made, decisions taken, resolutions passed, and any dissenting opinions at a Board meeting for a period, notwithstanding any requirements in any law or regulations, of not less than eight (8) years.

C. Board Remuneration Reporting Requirements

1. On an annual basis, VASPs providing Custody Services shall submit to VARA the following information—
 - a. details of all compensation and/or remuneration of all members of the Board and its committees, including but not limited to salaries, allowances, expenses, bonuses, benefits, or other incentive programmes (whether or not denominated in Virtual Assets). Such details shall include the type, nature and conditions of all such compensation and/or remuneration; and
 - b. reasons for all such compensation and/or remuneration.
2. All information submitted by VASPs in compliance with Rule I.C.1 of this Custody Services Rulebook shall be kept confidential by VARA, except to the extent that disclosure is required to comply with any applicable laws or regulations.

Part II – Policies, Procedures and Public Disclosures

A. Policies and Procedures

1. In addition to all other requirements in the Regulations and Rulebooks, VASPs providing Custody Services shall establish, implement and enforce appropriate written internal policies and procedures relating to the following—
 - a. the ability of clients to have access to and withdraw their Virtual Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility; and

- b. such other policies or procedures as VARA may require from time to time.
- 2. VASPs providing Custody Services shall assess and, in any case, at least yearly review the effectiveness of their policies and procedures, and take appropriate measures to address any deficiencies.

B. Public Disclosures

- 1. VASPs providing Custody Services shall publish on their website in a prominent place or make available by other publicly accessible means—
 - a. a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed;
 - b. their policies and procedures relating to data privacy, whistleblowing and handling of client complaints; and
 - c. a statement of whether the VASP has accounts, funds or Virtual Assets maintained by a third party and if so, provide the identity of that third party.]
- 2. Other disclosable matters. To the extent permissible under applicable laws, VASPs providing Custody Services shall publish on their website or by other publicly accessible means—
 - a. details of any past convictions or prosecutions of any member(s) of their Senior Management or Board, whether before the courts of the UAE or the courts of another jurisdiction; and
 - b. any such other information relating to their business or activities as VARA may reasonably require.
- 3. The disclosure requirements set out in this Rule II.B of this Custody Services Rulebook are in addition to all disclosures required under the Market Conduct Rulebook, and to all notifications to VARA required under the Compliance and Risk Management Rulebook.

Part III – VA Storage and Custody Rules

A. General Requirements

- 1. VASPs that provide Custody Services must comply with the provisions in this Part III of this Custody Services Rulebook.
- 2. To the extent any provisions are inconsistent with the Client VA Rules in the Compliance and Risk Management Rulebook, this Part III of this Custody Services Rulebook shall have precedence.
- 3. VASPs must ensure that all Custody Services are only provided in accordance with verified client instructions, or instructions from authorised agents of the client for whom the client has provided the VASP with a valid legal authority for the agent to provide instructions on the client's behalf.

B. Segregation and Control

- 1. Virtual Assets held by a VASP providing Custody Services are not depository liabilities or assets of the VASP.

2. VASPs shall not authorise or permit rehypothecation of Virtual Assets for which they provide Custody Services (regardless of whether they have obtained a client's consent), and VASPs providing Custody Services shall not seek or attempt to obtain such consent as part of the Custody Services they provide.
3. VASPs providing Custody Services shall segregate the Virtual Assets of each client in separate VA Wallets containing the Virtual Assets of that client only.
4. VASPs must maintain control of each Virtual Asset at all times while providing Custody Services.
5. VASPs providing Custody Services must be a separate legal Entity from any member of their Group that provides services relating to VA Activities other than Custody Services.
6. As a limited exception to Rule III.B.5, VASPs providing Custody Services may apply to VARA to obtain a Licence for the provision of VA Transfer and Settlement Services, which shall only be granted subject to VARA's satisfaction of all relevant requirements, including the VASP's implementation and strict enforcement of policies and procedures to achieve necessary segregation between operations relating to Custody Services and such VA Transfer and Settlement Services.
7. VASPs must have adequate policies and procedures to ensure that there is sufficient operational and physical segregation between individuals handling operations for Custody Services, and their other core businesses and operations including, but not limited to, other VA Activities conducted by their Group. Such policies and procedures shall establish a separate team to handle the VASP's Custody Services only, consisting of individuals who have no conflicting duties or access to information which may give rise to any conflicts of interest.

C. VA Wallet Management

1. Hot and cold Virtual Asset storage.
 - a. VASPs providing Custody Services shall at all times maintain appropriate certifications as may be required under industry best practices applicable to the safekeeping of Virtual Assets.
 - b. VASPs providing Custody Services should conduct a risk-based analysis to determine the method of Virtual Asset storage including different types of VA Wallets (e.g. hot versus cold storage).
 - c. VASPs providing Custody Services should document in detail, the methodologies and behaviour determining the transfer of Virtual Assets between different types of VA Wallets (e.g. hot, cold and warm wallets). The mechanisms for transfer between different types of VA Wallets should be well documented, and subject to internal controls and audits performed by an independent third-party auditor, ensuring compliance with Rule III.C.1.a of this Custody Services Rulebook.
2. Seed or key generation, storage, and use.
 - a. When creating any seed, asymmetric private and public key combinations, or other similar mechanisms required for providing Custody Services, VASPs shall use industry best standards to create the seed, asymmetric private and public key combinations, or other similar mechanisms to ensure a secure generation mechanism. In addition, all VASPs providing Custody Services shall consider all risks associated with producing a private key or seed for a signatory including whether the signatory should be involved in the generation process or whether creators of the seed, private key, or other similar mechanism should be prohibited from cryptographically signing any transaction or from having access to any relevant systems.

- b. VASPs providing Custody Services shall adopt industry best practices when using encryption, and secure device storage for a client's private keys when not in use. VASPs must ensure that any keys stored online or in one physical location are not capable of conducting a Virtual Asset transaction, unless appropriate controls are in place to ensure that physical access itself by an individual is insufficient to conduct a transaction.
- c. All key and seed backups must be stored in a separate location from the primary key and seed. Key and seed backups must be stored with encryption at least equal to the encryption used to protect the primary seed and key. If VASPs use mnemonic back-up seed phrases, it should ensure that the mnemonic back-up seed phrase is broken into at least two (2) parts. Any backups that when combined could facilitate a transaction, must not be stored in a single point of access.
- d. VASPs providing Custody Services should consider using multi-signature approaches where appropriate. VARA reserves the right to require VASPs to use multi-signature approaches in specific situations, including for specific types of Virtual Assets. If a VASP has multi-signature arrangements that vary depending on the risk of the transaction, the VASP must have well-documented and audited procedures.
- e. VASPs providing Custody Services must mitigate the risk of collusion between all authorised parties or signatories who are able to authorise the movement, transfer or withdrawal of Virtual Assets held under custody on behalf of clients. The risk of collusion and other internal points of failure should be evaluated for materiality and probability, and effectively addressed during recurring operational risk assessments.

3. Lost or stolen keys.

- a. VASPs providing Custody Services shall establish, and maintain effective policies and procedures in the event that any seed or cryptographic keys of any VA Wallet are lost or otherwise compromised. Such policies and procedures shall address matters including but not limited to—
 - i. recovery of affected Virtual Assets;
 - ii. timely communications with all clients and counterparties regarding consequences arising from relevant incidents, and measures being taken to remedy such consequences;
 - iii. cooperation with law enforcement agencies and regulatory bodies; and
 - iv. if applicable, preparation of wind-down arrangements and public disclosure of such arrangements.

D. Additional Obligations

1. Written agreements with clients.

- a. In addition to all applicable requirements in the Market Conduct Rulebook, Client Agreements entered into between VASPs providing Custody Services and clients should include the following—
 - i. description of the overall custodial framework used by the VASP when providing Custody Services, including but not limited to security, risk mitigation, safeguarding procedures;
 - ii. address what will happen when source code versions underlying a Virtual Asset supported by the VASP materially change in a way that may affect the Custody

Services provided (e.g. a ‘fork’ of the network protocol), including but not limited to—

1. notification requirements if the VASP will not support the original source code version;
2. notification requirements if the VASP will support the original source code version;
3. notification requirements if the original source code version will no longer exist, or is not reasonably expected to continue to exist, or if the original source code version will no longer function securely and/or as originally intended; and
4. actions that will be taken by the VASP if any/all of the above were to take place;

- iii. when and how the Virtual Assets under custody will be returned;
- iv. settlement finality, including when a Virtual Asset will be deemed fully transferred, and the VASP discharged of any obligations upon transfer of the Virtual Asset (including but not limited to withdrawals initiated by the client);
- v. the frequency of account statements to be provided to clients, and the content of those statements;
- vi. who (e.g. the VASP, its agent or another third party) is responsible for securing the Virtual Assets, and protecting them from theft or loss;
- vii. the VASP’s Outsourcing practices including, if the VASP Outsources some or all of the Custody Services to third parties, the qualifications of those third parties;
- viii. the VASP’s cybersecurity and data privacy policies, procedures, controls and systems, including how the VASP will respond to data breaches and cyberattacks, and notification, reimbursement and remediation policies; and
- ix. the VASP’s policies and procedures for safeguarding access to Virtual Assets, including policies and procedures related to multi-signature/multi-key safeguards, access management controls, and revocation of key signatories’ access.

2. Relationship between a VASP and client, for the provision of Custody Services.
 - a. The provision of Custody Services shall be a contractual arrangement between a VASP and a client, under which a client lawfully in control of, or entitled to control, a Virtual Asset, transfers control of the Virtual Asset to a VASP, solely for the purpose of receiving the Custody Services, and does not in any way transfer to the VASP, any legal interest in the Virtual Asset, or any discretionary authority not explicitly authorised in the Client Agreement or otherwise agreed to by the client.
 - b. In addition to all Reserve Assets requirements in the Company Rulebook, VASPs providing Custody Services will keep a register, and record of reconciliation of each client’s positions that correspond to the client’s rights to the Virtual Assets that are subject to the Custody Services.
3. Outsourcing and third-party suppliers.
 - a. If a VASP Outsources some or all of the Custody Services to third parties, the VASP is responsible for ensuring that all applicable laws, Regulations, Rules and Directives are complied with.
 - b. VASPs must have established roles and responsibilities for its Custody Services operations, and its operational risk management. The responsibility for manually executed core functions of Custody Services, should only be performed by authorised employees.

4. Account statements. VASPs providing Custody Services must provide at least every month, and promptly at the request of a client, a statement with all Virtual Asset transactions specific to each client account, the dates and transaction amounts of the corresponding transactions, and balances and value for each type of Virtual Asset.
5. Audit. VASPs should maintain a full audit trail of all transaction activities that occur on a client's account for at least eight (8) years. The audit trail should include specific information regarding each transaction, such as the date and time, the transaction type, the relevant signatories, and the Virtual Assets involved.

Part IV – Staking from Custody Services Rules

A. Compliance with Staking from Custody Services Rules

1. VASPs Licensed by VARA to carry out Custody Services may only provide Staking from Custody Services, if explicitly authorised to do so by VARA, and such authorisation is expressly stipulated in their Licence. VASPs will be subject to licensing and/or supervision fees incremental to the fees for Custody Services in Schedule 2 of the Regulations, or other fees published by VARA, as amended from time to time, in order to be able to undertake the regulated activity of Staking from Custody Services.
2. VASPs that are authorised to provide Staking from Custody Services must comply with this Part IV of this Custody Services Rulebook, at all times, when providing these services.
3. Staking from Custody Services is regarded by VARA to form part of the Custody Services that a VASP provides. As such, all VASPs providing Staking from Custody Services must continue to comply with all other Rules relating to Custody Services throughout the provision of Staking from Custody Services, for all Virtual Assets to which the Staking from Custody Services relate.
4. For the avoidance of doubt, VASPs Licensed by VARA to carry out Custody Services that are also authorised to provide Staking from Custody Services, may only provide Staking from Custody Services for Virtual Assets for which they are providing Custody Services.
5. VASPs Licensed by VARA to carry out Custody Services that are also authorised to provide Staking from Custody Services, may provide Staking from Custody Services through the same legal Entity. For avoidance of doubt, such authorisation for, and provision of Staking from Custody Services is considered to be sub-set of the Custody Services Activity, and is hence not subject to the requirement for a separate legal Entity stipulated under Rule III.B.5 of this Custody Services Rulebook.
6. VARA shall have the right to suspend or revoke any authorisation granted to a VASP to provide Staking from Custody Services, in respect of any specific DLT, or in its entirety across all DLTs, upon reasonable grounds VARA deems appropriate.

B. Client instructions

1. VASPs providing Staking from Custody Services must comply with Rule III.A.3 of this Custody Services Rulebook, and continue to act only on explicit instructions received from their clients throughout the provision of such services, including when they are required to vote or otherwise participate in the governance of any DLT on behalf of their clients.
2. If a VASP wishes to obtain and rely on any pre-authorised instruction from a client, the VASP must consider all reasonably foreseeable circumstances where such instruction is likely to be used by the VASP as authorisation, and the VASP must communicate all such circumstances clearly to the client, prior to the client providing such instruction. All pre-authorised instructions sought or obtained by a VASP must be sufficiently detailed, accurate and relevant for the client to

understand both the circumstances in, and actions for which such instructions will be relied upon by the VASP.

3. Staking from Custody Services cannot be provided on an 'opt-out' basis, and the activity may only be initiated after the VASP has received a client's specific instruction to do so.

C. Segregation and safekeeping of Virtual Assets

1. Segregated client VA Wallets. VASPs providing Staking from Custody Services must ensure that each client's Virtual Assets remain segregated in separate VA Wallets containing the Virtual Assets of that client only, throughout the provision of such Staking from Custody Services, as required under Rule III.B.3 of this Custody Services Rulebook.
2. Single client per node. VASPs providing Staking from Custody Services must ensure that no client's Virtual Assets are pooled or otherwise combined with Virtual Assets of any other clients of the VASP or any other party(ies), whether to meet any minimum requirements of a given DLT or otherwise, and each node or instance of a DLT managed, operated or otherwise made available by the VASP may only hold, be delegated, or have committed to it, Virtual Assets belonging to that client only.
3. Safekeeping of Virtual Assets. VASPs providing Staking from Custody Services remain responsible to their clients for the safekeeping of the Virtual Assets for which Staking from Custody Services is being provided.
4. Control of withdrawal keys. VASPs providing Staking from Custody Services must maintain control of the cryptographic keys and/or other mediums or methods through which the Virtual Assets may be withdrawn, or otherwise no longer 'staked'.

D. Node management

1. VASPs providing Staking from Custody Services must use all commercially reasonable endeavours to ensure all operational, maintenance or other requirements for participation (including, but not limited to, hardware, software, connectivity and upgrades of the same) determined by the relevant DLT are met in respect of Staking from Custody Services, in order to minimise the risk of 'slashing' or other penalties being incurred in respect of the Virtual Assets, for which the VASP is providing such Staking from Custody Services.
2. VA Wallet management. VASPs providing Staking from Custody Services shall continue to comply with all requirements in Rule III.C of this Custody Services Rulebook, and the above Rule IV.D.1 of this Custody Services Rulebook applies in addition to those requirements.
3. Outsourcing. In addition to the requirements in Rule III.D.3 of this Custody Services Rulebook, VASPs shall ensure that all third-party services used by the VASP in the provision of Staking from Custody Services, comply with Part IV of the Company Rulebook.

E. DLT Standards

1. VASPs providing Staking from Custody Services shall establish standards for the DLTs for which it provides, or the DLTs it uses to provide Staking from Custody Services ("**DLT Standards**").
2. DLT Standards shall include, but not be limited to—
 - a. security and immutability of the DLT protocol, including its level of centralisation, reliance on a single Entity, or any potential single points of failure;
 - b. operating history of the DLT, including any periods of disruption or downtime;
 - c. soundness of the staking protocol and operation, including the duration for which it has successfully been active;

- d. source of any rewards being offered by the DLT or any other party for a user's participation, including whether such rewards are derived from the fees paid by users of the DLT, or from other means;
- e. the VASP's ability to maintain all operational, maintenance or other requirements for participation;
- f. its design, features and use cases, whether or not intended by relevant developers;
- g. any features that present a risk of materially affecting the VASP's compliance with applicable laws, Regulations, Rules or Directives, including but not limited to those relating to AML/CFT, sanctions, security and intellectual property;
- h. regulatory treatment by VARA and other appropriate authorities (including those outside of the Emirate);
- i. future development plans (e.g. 'roadmap') of the DLT as communicated by relevant developers, and whether such developments may have an impact (positive or negative) on, or relevance to, any of the above factors;
- j. potential or actual conflicts of interest that may arise should the VASP provide any Staking from Custody Services in relation to the DLT, and relevant mitigations provisioned for such instances;
- k. background of the founders, management, and current core developers of the DLT, including, but not limited to, relevant experience in the Virtual Asset sector, and whether they have been subject to any investigations, penalties, or claims in relation to fraud or deceit etc.; and
- l. any additional factors that the VASP may require to be considered.

3. VASPs providing Staking from Custody Services shall take all reasonable steps, including but not limited to conducting relevant due diligence, prior to the provision of such services in respect of a DLT, to ensure the DLT meets all their prescribed DLT Standards.

4. VASPs providing Staking from Custody Services must actively monitor all DLTs for which Staking from Custody Services is provided, for continued compliance with their DLT Standards.

5. Upon becoming aware that a DLT no longer meets a VASP's prescribed DLT Standards, the VASP must—

- a. notify all affected clients and VARA immediately;
- b. cease accepting new Virtual Assets for Staking from Custody Services in respect of that DLT immediately;
- c. determine a course of action with such affected clients to cease all Staking from Custody Services for that DLT, as soon as practicable;
- d. continue to provide such Staking from Custody Services in accordance with this Part IV of this Custody Services Rulebook throughout the agreed course of action, and until such services have been effectively concluded;
- e. keep VARA informed of all actions being taken throughout such course of action; and
- f. take all other steps as VARA may direct.

6. VASPs providing Staking from Custody Services shall also set and implement conditions, under which the VASP will suspend accepting new Virtual Assets for Staking from Custody Services which, as required under Rule IV.E.5 of this Custody Services Rulebook above, must include where a DLT no longer meets the VASP's DLT Standards.

7. VASPs must maintain all records relevant to such assessments under this Rule IV.E of this Custody Services Rulebook for eight (8) years, and provide such records for VARA's inspection upon request..

F. Risk disclosure statement

1. VASPs providing Staking from Custody Services must provide each client with a risk disclosure statement explaining (i) that Virtual Assets for which Staking from Custody Services is being provided, may be at risk of loss, reduction or penalty, (ii) the types and nature of such risks, (iii) the circumstances in which such risks may arise, and (iv) the likelihood and severity of consequences that may be suffered.
2. The risk disclosure statement required under Rule IV.F.1 above of this Custody Services Rulebook must be separate from the Client Agreement, and VASPs must independently obtain confirmation of the acceptance of such risk disclosure statement from each client, prior to the VASP providing Staking from Custody Services to that client.

G. Client Agreements

1. In addition to all requirements in respect of Client Agreements in the Market Conduct Rulebook, and under Rule III.D of this Custody Services Rulebook, VASPs providing Staking from Custody Services shall include the following, to the extent applicable, in Client Agreements in respect of Staking from Custody Services—
 - a. a description of the Virtual Assets for which Staking from Custody Services is being provided to such extent that the details are sufficient to identify them;
 - b. operational, maintenance or other requirements for participation (including but not limited to hardware, software and connectivity) of the DLT(s), for which Staking from Custody Services is being provided, and that the VASP undertakes the responsibility to meet those requirements when providing such services. This Rule IV.G.1.b of the Custody Services Rulebook can be largely met by providing links to publicly available sources of where such information is officially maintained, for example, DLT website or source code repository etc.;
 - c. respective rights of the VASP, the client and any other Entity involved in the Staking from Custody Services, in respect of Virtual Assets that are the subject of the Client Agreement;
 - d. a detailed description of the source of all rewards received by clients from the Staking from Custody Services, including whether such rewards are generated solely from fees paid by users of the DLT, or whether such rewards are derived from any other source;
 - e. proceeds to be paid or become payable, and in the case of variable proceeds, the method of calculation, factors that impact the amount, volatility and timing of the proceeds, and how and when such variations will be communicated by the VASP to its clients, including all rights that the client has to influence decisions at each stage;
 - f. all fees to be charged for Staking from Custody Services, and the calculation thereof;
 - g. rights of the client to withdraw or directly control decisions pertaining to any Virtual Assets, in respect of which Staking from Custody Services is provided, and any conditions/ circumstances under which the client may be unable to do so;
 - h. statement explaining that Virtual Assets in respect of which Staking from Custody Services is provided may be at risk, including the types and nature of such risks, as well as the likelihood and severity of any losses that may be suffered;
 - i. rights, if any, of the VASP to vary the terms of the Client Agreement;
 - j. rights of the VASP and the client to terminate the Client Agreement, circumstances under which these rights can be activated, and the consequences of such termination;
 - k. full details of the VASP's client complaints procedure; and
 - l. statement explaining whether the VASP receives any remuneration, discount or other benefit for using any third party (with a disclosure of specific Entities where applicable), in

the course of the provision of the Staking from Custody Services.

Part V – Collateral Wallet Services Rules

A. Compliance with Collateral Wallet Services Rules

1. Only VASPs Licensed by VARA to carry out Custody Services may provide Collateral Wallet Services.
2. VASPs Licensed by VARA to carry out Custody Services may only provide Collateral Wallet Services if explicitly authorised to do so by VARA, with such authorisation being expressly stipulated in the VASP's Licence.
3. VASPs providing Collateral Wallet Services will be subject to licensing and/or supervision fees incremental to the fees for Custody Services in Schedule 2 of the Regulations, or other fees published by VARA, as amended from time to time, in order to be able to provide Collateral Wallet Services.
4. VASPs that are authorised to provide Collateral Wallet Services must comply with this Part V of the Custody Services Rulebook, at all times, when undertaking the regulated activity of providing Collateral Wallet Services.
5. Collateral Wallet Services are regarded by VARA as ancillary services to the Custody Services that a VASP provides. As such, all VASPs providing Collateral Wallet Services must comply with all other Rules relating to Custody Services throughout the provision of Collateral Wallet Services, including but not limited to the Client Virtual Assets Rules in Part V of the Compliance and Risk Management Rulebook, subject only to the explicit exceptions contained in this Part V of the Custody Services Rulebook.
6. In addition to VARA's powers in Part IX of the Regulations, VARA shall have the right to limit, suspend or revoke any authorisation granted to a VASP to provide Collateral Wallet Services, upon reasonable grounds VARA deems appropriate at any time.

B. Client Instructions

1. VASPs providing Collateral Wallet Services must comply with Rule III.A.3 of this Custody Services Rulebook and continue to act only on explicit instructions received from their clients throughout the provision of such services.
2. If a VASP wishes to obtain and rely on any pre-authorised instruction from a client, the VASP must consider all reasonably foreseeable circumstances where such instruction is likely to be used by the VASP as authorisation, and the VASP must communicate all such circumstances clearly to the client, prior to the client providing such instruction.
3. All pre-authorised instructions sought or obtained by a VASP must be sufficiently detailed, accurate and relevant for the client to understand both the circumstances in, and actions for, which such instructions will be relied upon by the VASP.
4. Collateral Wallet Services cannot be provided on an 'opt-out' basis, and the activity may only be initiated after the VASP has received a client's specific instruction to do so.

C. Receipts

1. Immediately after receiving a client's instructions to initiate a transfer of Virtual Assets to an account and/or VA Wallet for the purposes of Collateral Wallet Services, a VASP must provide the client with a receipt including the following information—

- a. confirmation of whether the transfer has been successfully initiated;
 - b. date and time of receipt of the client's instructions;
 - c. amount and type of Virtual Assets in the transfer;
 - d. transaction identification details and/or reference; and
 - e. total balance of the client's Virtual Assets held in the client's account and/or VA Wallet for the purposes of Collateral Wallet Services.
2. Immediately after a transaction on the account and/or VA Wallet used for the provision of Collateral Wallet Services has been completed, a VASP must provide the client with a receipt including the following information—
 - a. date and time of the transaction;
 - b. details of the recipient including whether the transaction has been credited back to the client or to an Exchange;
 - c. amount and type of Virtual Assets in the transaction;
 - d. transaction identification details and/or reference;
 - e. full details of all exchanges, trades or conversions completed in the course of the transaction (if applicable), including times and rates of the exchange;
 - f. a breakdown of all fees paid or payable by the client and when they have been paid or become payable (as applicable); and
 - g. total balance of the client's Virtual Assets held in the client's account and/or VA Wallet for the purposes of Collateral Wallet Services.

D. VA Wallets and Safekeeping of Virtual Assets

1. VASP must use VA Wallets which are specifically designated for the purposes of providing Collateral Wallet Services only ("CWS Client VA Wallet"). VASPs must identify CWS Client VA Wallets used for providing Collateral Wallet Services as such in their internal books and records. CWS Client VA Wallets used for providing Collateral Wallet Services cannot be re-purposed or used for any other purpose either during or after the provision of Collateral Wallet Services.
2. As a limited exception only, Rule III.B.3 of this Custody Services Rulebook shall not apply to the CWS Client VA Wallets used by the VASP for the provision of Collateral Wallet Services.
3. VASPs providing Collateral Wallet Services remain responsible to their clients for the safekeeping of the Virtual Assets for which Collateral Wallet Services are being provided.

E. Settlement integration with trading venues

1. VASPs providing Collateral Wallet Services may only provide the Collateral Wallet Services to their clients for trading or other transactions on venues which are Licensed by VARA to carry out Exchange Services ("Exchange").
2. VASPs providing Collateral Wallet Services may only provide the Collateral Wallet Services in respect of one Exchange per client account and/or VA Wallet. A VASP's client may have multiple accounts and/or VA Wallets with the VASP through which Collateral Wallet Services are provided, in order for the client to trade or transact on different Exchanges, however each account and/or VA Wallet may only be in respect of one Exchange.
3. Further to Rule V.E.2 of this Custody Services Rulebook above, VASPs providing Collateral Wallet Services may only permit one Exchange to have any rights or claims over Virtual Assets held in any given CWS Client VA Wallet used for the provision of the Collateral Wallet Services.

4. In addition to all requirements under Part II.C of the Company Rulebook, VASPs providing Collateral Wallet Services must identify and disclose all conflicts of interest between the VASP and its clients in the provision of the Collateral Wallet Services including, but not limited to, any conflicts which arise because of the VASP's commercial arrangements with any Exchange.

F. Risk Disclosure Statement

1. VASPs providing Collateral Wallet Services must provide each client with a risk disclosure statement in respect of the Collateral Wallet Services explaining—
 - a. co-mingling of Client VAs. To the extent applicable, that Client VAs may no longer be held in segregated VA Wallets containing the Virtual Assets of that client only;
 - b. safekeeping. A detailed description of how Client VAs are held, including but not limited to if Client VAs are held in accounts and/or VA Wallets containing Virtual Assets of more than one client of the VASP; and
 - c. rights of Exchanges. The nature of all rights or claims that any Exchange has over Client VAs, accounts, Client VA Wallets and/or any CWS Client VA Wallet.
2. The risk disclosure statement required under Rule V.F.1 above of this Custody Services Rulebook must be separate from the Client Agreement and VASPs must independently obtain confirmation of the acceptance of such risk disclosure statement from each client, prior to the VASP providing Collateral Wallet Services to that client.

G. Client Agreements

1. In addition to all requirements in respect of Client Agreements in the Market Conduct Rulebook, and under Rule III.D of this Custody Services Rulebook, VASPs providing Collateral Wallet Services shall include the following, to the extent applicable, in Client Agreements in respect of the Collateral Wallet Services—
 - a. a description of the Virtual Assets for which Collateral Wallet Services are provided to such extent that the details are sufficient to identify them;
 - b. respective rights of the VASP, the client and any other Entity involved in the Collateral Wallet Services, in respect of Virtual Assets that are the subject of the Client Agreement;
 - c. rights of the client to withdraw, manage or directly control decisions pertaining to any Virtual Assets, in respect of which the Collateral Wallet Services are provided, and any conditions or circumstances under which the client may be unable to do so;
 - d. a statement explaining that Virtual Assets in respect of which the Collateral Wallet Services are provided may be at risk, including the types and nature of such risks, as well as the likelihood and severity of any losses that may be suffered; and
 - e. a statement explaining whether the VASP receives any remuneration, discount or other benefit for using any third party (with a disclosure of the specific Entities where applicable), in the course of the provision of the Collateral Wallet Services.

H. Reporting and Notification

1. Reporting. In addition to all other applicable requirements in respect of regulatory reporting in the Regulations, Rulebooks or its Licence, VASPs providing Collateral Wallet Services shall, on a

monthly basis, submit to VARA the following information—

- a. in respect of the Client Virtual Assets held in CWS Client VA Wallets used for the provision of the Collateral Wallets Services—
 - i. a list of all Virtual Assets held in the and the total number held of each Virtual Asset; and
 - ii. the total value, denominated in AED, for each Virtual Asset listed in Rule V.H.1.a.i of this Custody Services Rulebook;
- b. total number of clients to whom the VASP provides or has provided the Collateral Wallets Services in the relevant reporting period; and
- c. the names of each of the Exchanges with whom the VASP has settlement integrations and/or who have any rights or claims over any CWS Client VA Wallet, in accordance with Rule V.E.

2. Notifications. In addition to all other notification requirements in the Regulations, Rulebooks or its Licence, VASPs providing Collateral Wallet Services shall notify VARA immediately in the event of any of the following, at any time during the provision of the Collateral Wallet Services—

- a. system, reporting or reconciliation delay or failure; and
- b. an error or inaccuracy in the recording of any client's balance.

Schedule 1— Definitions

Term	Definition
“Client Agreements”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Collateral Wallet Services”	means the provision of accounts and/or VA Wallets, containing Client's Virtual Assets, which are used to facilitate net settlement of clients' positions between a VASP Licensed by VARA to provide Custody Services and a VASP Licensed by VARA to carry out Exchange Services.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Custody Services”	has the meaning ascribed to it in Schedule 1 of the Regulations.
“Custody Services Rulebook”	means this Custody Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“CWS Client VA Wallet”	has the meaning ascribed to it in <u>Rule V.D.1</u> of this Custody Services Rulebook.
“Directive”	has the meaning ascribed to it in the Regulations.
“DLT Standards”	has the meaning ascribed to it in <u>Rule IV.E.1</u> of this Custody Services Rulebook.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.

“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Exchange”	has the meaning ascribed to it in <u>Rule V.E.1</u> of this Custody Services Rulebook.
“Group”	has the meaning ascribed to it in the Company Rulebook.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means holding a valid Licence.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Outsourcing”	has the meaning ascribed to it in the Company Rulebook.
“Paid-Up Capital”	has the meaning ascribed to it in the Company Rulebook.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Reserve Assets”	has the meaning ascribed to it in the Company Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Staking from Custody Services”	means ‘staking’ or otherwise using, committing, pledging or locking up Virtual Assets, for which the VASP is providing Custody Services, for the purposes of participating in the consensus mechanisms or other maintenance, operation or functioning of a DLT to which those Virtual Assets relate, and may include receiving rewards generated and distributed for that participation.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity Licensed by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.
“VA Wallet”	has the meaning ascribed to the term “Virtual Asset Wallet” in the Dubai VA Law.

Exchange Services Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Exchange Services Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time ("Regulations"), issued by VARA, and applies to all VASPs Licensed by VARA to carry out Exchange Services in the Emirate.

This Exchange Services Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out Exchange Services must also comply with the following Rulebooks applicable to all VASPs—

1. Company Rulebook;
2. Compliance and Risk Management Rulebook;
3. Technology and Information Rulebook;
4. Market Conduct Rulebook; and
5. All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

For the avoidance of doubt, where a VASP is Licensed by VARA to carry out other VA Activities in the Emirate in addition to Exchange Services, it must comply with all Rulebooks which apply to those other VA Activities. Unless otherwise stated, the Rules in VA Activity specific Rulebooks apply cumulatively for each VA Activity a VASP carries out.

Capitalised terms in this Exchange Services Rulebook have the meanings ascribed to them in the Regulations or as otherwise defined herein or provided in Schedule 1.

Part I – Additional Board Requirements

A. Board Constitution

1. The Board of a VASP providing Exchange Services shall consist of executive directors and non-executive directors, with a minimum of one (1) director qualifying as an independent director as set out below.
2. The Board of a VASP providing Exchange Services shall convene at least on a quarterly basis.
3. VASPs providing Exchange Services shall mandate the length of each term and number of terms each Board member may serve on the Board.
4. A Board member is not regarded as an independent director of a VASP if—
 - a. they or any of their first degree relatives are working or have worked as a member of the Senior Management, or held a role in the VASP's Group equivalent to Senior Management within the preceding two (2) years preceding the date of their nomination to the Board;
 - b. they or any of their first degree relatives have a direct or indirect interest in the contracts and projects concluded with the Group during the preceding two (2) years, provided that the aggregate value of such contracts and projects do not exceed the lower of (i) ten percent (10%) of the Paid-Up Capital of the VASP or (ii) the amount of AED 5,000,000 or its equivalent in other foreign currency, unless such contracts and projects relate to the ordinary course of business of the VASP and do not contain any preferential conditions;
 - c. they are working or have worked for the Group during the preceding two (2) years preceding the date of their appointment to the Board;
 - d. they work for, or are a partner of, a company that performs consultancy services for the VASP or any members of its Group, or has performed such services during the preceding two (2) years;

- e. they have any personal service contracts with the VASP or any members of its Group, or have had such contract during the preceding two (2) years, excluding any contract under which they are appointed as a non-executive director;
- f. they are directly or indirectly linked to any Entity that receives substantial funding from the VASP's Group;
- g. they or any of their first degree relatives are a partner or an employee of the auditor of the VASP, or if, during the preceding two (2) years preceding the date of their Board membership, were a partner or an employee of the auditor of the VASP;
- h. the ownership held by them and their first degree relatives reaches ten percent (10%) or more of the share capital of the VASP;
- i. they have served more than seven (7) years as a Board member of the VASP; or
- j. they are the representative of an investor in the VASP holding ten percent (10%) or more of the share capital of the VASP.

B. Board Committees

- 1. The Board of a VASP providing Exchange Services shall establish remuneration, nomination and audit committees, and may establish additional committees to perform certain delegated functions on behalf of the Board. The Board may delegate specific authority, but not its responsibilities, to its committees, provided that it continuously monitors and oversees the work conducted by all committees.
- 2. Each committee created by the Board of a VASP providing Exchange Services shall—
 - a. have a charter or other instrument that sets out its membership, mandate, scope, working procedures and means of accountability to the Board; and
 - b. report to the Board on findings and recommendations relating to the work entrusted by the Board to it regularly.
- 3. The Board and its committees shall keep minutes to record details of the matters discussed, recommendations made, decisions taken, resolutions passed and any dissenting opinions at a Board meeting for a period of, notwithstanding any requirements in any law or regulations, not less than eight (8) years.

C. Board Remuneration Reporting Requirements

- 1. On an annual basis, VASPs providing Exchange Services shall submit to VARA the following information—
 - a. details of all compensation and/or remuneration of all members of the Board and its committees, including but not limited to salaries, allowances, expenses, bonuses, benefits, or other incentive programmes (whether or not denominated in Virtual Assets). Such details shall include the type, nature and conditions of all such compensation and/or remuneration; and
 - b. reasons for all such compensation and/or remuneration.
- 2. All information submitted by VASPs in compliance with Rule I.C.1 of this Exchange Services Rulebook shall be kept confidential by VARA, except to the extent that disclosure is required to comply with any applicable laws or regulations.

Part II – Policies, Procedures and Public Disclosures

A. Policies and Procedures

1. In addition to all other requirements in the Regulations and Rulebooks, VASPs providing Exchange Services shall establish, implement and enforce appropriate written internal policies and procedures relating to the following—
 - a. the prohibition, detection, prevention and/or deterrence of Market Offences and any other abusive practices within their business or using their services, including but not limited to relevant internal rules, compliance programmes, sanctioning policies and powers;
 - b. the ability of clients to have access to and withdraw their Virtual Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility;
 - c. settlement, delivery and clearing;
 - d. establishing and amending the method of determining the price of Virtual Assets, including the use of market data to ensure the integrity and reliability of the determined price; and
 - e. such other policies and procedures as VARA may require from time to time.
2. VASPs providing Exchange Services shall assess and, in any case, at least yearly review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.

B. Public Disclosures

1. VASPs providing Exchange Services shall publish on their website in a prominent place or make available by other publicly accessible means—
 - a. a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed;
 - b. their policies and procedures relating to data privacy, whistleblowing and handling of client complaints;
 - c. a summary containing the following information pertaining to each Virtual Asset offered for exchange by the VASP—
 - i. name and symbol;
 - ii. date of issuance;
 - iii. market capitalisation and fully diluted value;
 - iv. circulating supply, including as a percentage of maximum total supply (if applicable);
 - v. whether the Virtual Asset has been subject to an independent smart contract audit and the date of the most recent audit; and
 - vi. largest reduction in price from high to low stated as both an absolute amount and a percentage change, including when it occurred;
 - d. details of how Virtual Assets traded over their trading venues are deposited and protected and how clients' ownership in respect of those Virtual Assets are thereby respected; and
 - e. a description of how the VASP determines the prices of the Virtual Assets it quotes to clients.

2. Other disclosable matters. To the extent permissible under applicable laws, VASPs providing Exchange Services shall publish on their website or by other publicly accessible means—
 - a. details of any past convictions or prosecutions of any member(s) of their Senior Management or Board, whether before the courts of the UAE or the courts of another jurisdiction; and
 - b. any such other information relating to their business or activities as VARA may reasonably require.
3. The disclosure requirements set out in this Rule II.B of the Exchange Services Rulebook are in addition to all disclosures required under the Market Conduct Rulebook and to all notifications to VARA required under the Compliance and Risk Management Rulebook.

Part III – Exchange Services Rules

A. Trading Venue Participants and Code of Conduct

1. VASPs providing Exchange Services shall publish and enforce a code of conduct or other rules for all participants on their trading venue.
2. The code of conduct required under Rule III.A.1 of this Exchange Services Rulebook should provide VASPs the rights and/or power to implement disciplinary actions against participants on their trading venue where they breach any Regulations, Rules or Directives.
3. VASPs providing Exchange Services shall ensure that the code of conduct provides them the necessary rights and/or powers to issue, impose, require or collect, the following—
 - a. warnings;
 - b. reprimands;
 - c. training;
 - d. qualification minimums;
 - e. remediation plans;
 - f. compliance audits;
 - g. restitution;
 - h. contractually agreed penalties;
 - i. conditions on trading;
 - j. trading prohibitions;
 - k. suspensions and restrictions to trading;
 - l. expulsions;
 - m. cancellation of a client's orders and any outstanding instructions from that client;
 - n. report any breaches to VARA; and
 - o. criminal referrals.
4. VARA shall have authority to pursue such additional remedies or disciplinary measures against participants of the trading venue of a VASP providing Exchange Services as it determines and may, in its sole and absolute discretion, delegate to a VASP providing Exchange Services the ability to enforce such additional remedies or disciplinary measures upon its written consent.
5. In addition to the above, VARA may require the suspension of trading of any Virtual Asset with effect from such time as it may determine, if there are reasonable grounds to suspect non-compliance with this Part III of the Exchange Services Rulebook. If VARA has required the

suspension of trading of any Virtual Asset, it may impose such conditions on the procedure for lifting the suspension as it considers appropriate.

6. VASPs providing Exchange Services shall ensure that—

- a. their code of conduct or other rules with respect to the conduct of their clients and trading venue participants are fairly disclosed to all relevant Entities; and
- b. clients provide valid acceptance to such rules in the Client Agreement in accordance with applicable laws.

B. Market Surveillance and Notifications to VARA

1. VASPs providing Exchange Services shall share information for surveillance and disciplinary purposes with VARA, including establishing arrangements that allow the VASP to share information on large exposures in correlated markets.
2. If a VASP suspects potential abuse affecting the market, the following information shall be provided to VARA, as applicable—
 - a. details of a participant's positions, in particular details of any large positions held, including on-exchange, related 'over-the-counter' derivatives and physical market positions;
 - b. Virtual Asset inventory levels;
 - c. delivery mode and forms of service;
 - d. action taken to implement position management powers;
 - e. changes to position limits;
 - f. additional Margin calls; and
 - g. other action taken by the VASP.
3. VASPs providing Exchange Services shall ensure that their fee structures are transparent, fair and non-discriminatory and that they do not create incentives to place, modify or cancel orders or to execute transactions in a way that disrupts the fair and orderly functioning of any market involving Virtual Assets.

C. Trading Systems Continuity

1. In addition to all requirements in the Technology and Information Rulebook, VASPs providing Exchange Services shall have in place effective systems, procedures and arrangements to ensure that their trading systems—
 - a. are resilient;
 - b. have sufficient capacity to ensure orderly trading under conditions of high uncertainty and/or extreme volatility;
 - c. are able to reject orders that exceed pre-determined volume and price thresholds or are clearly erroneous;
 - d. are fully tested to ensure that conditions under Rules III.C.1.a-c of this Exchange Services Rulebook are met; and
 - e. are subject to effective business continuity arrangements including, but not limited to, back-up and/or disaster recovery systems, facilities and sites, to ensure continuity of their services and reporting ability if there is any failure of the trading system.

D. Settlement

1. VASPs providing Exchange Services shall complete the final settlement of a Virtual Asset transaction within twenty-four (24) hours of the transaction being executed on their trading venues, subject to any factors outside the VASP's control, including but not limited to any limitations or malfunctioning of any DLT not controlled by the VASP or its Group.

Part IV – Margin Trading Rules

A. Compliance with Margin Trading Rules

1. VASPs may only provide Margin Trading services if explicitly authorised to do so by VARA and such authorisation is expressly stipulated in their Licence.
2. VASPs that are authorised to provide Margin Trading services, must comply with this Part IV of the Exchange Services Rulebook at all times when providing Margin Trading services.
3. VASPs must ensure that they have sufficient assets to provide Margin Trading services in order that they can fully satisfy client obligations, at all times.

B. VARA Approval and Powers

1. VARA may approve an application for the provision of Margin Trading services, provided that the VASP can demonstrate, to VARA's satisfaction, compliance with the following requirements—
 - a. the VASP has submitted for VARA's approval details of the terms and conditions upon which it proposes to offer Margin Trading services to clients, including a copy of the template Margin Trading Agreement to be used by the VASP, together with information relating to the VASP's financial condition and compliance with all Capital and Prudential Requirements applicable to the VASP;
 - b. the VASP has established, and is able to demonstrate to VARA upon request, appropriate policies and procedures as well as systems and controls with regards to Margin Trading services, which shall include but not be limited to—
 - i. the Margin which may be called, the applicable Margin rates and the method of calculating the Margin;
 - ii. the acceptable methods of Margin payment and forms of collateral;
 - iii. the circumstances under which a client or counterparty may be required to provide Margin and additional Margin, and the consequences of a failure to meet a Margin call, including the actions which the VASP may be entitled to take; and
 - iv. applicable escalation procedures where a client or counterparty fails to meet Margin calls; and
 - c. the VASP ensures, and is able to demonstrate to VARA upon request, that Virtual Assets collected as collateral for Initial Margin and Maintenance Margin purposes are liquid and can be liquidated within a reasonable timeframe.
2. VARA may request to inspect the Margin Trading system of the VASP used to calculate clients' Margin Trading positions and Margin and, prior to granting approval, request any other clarifications, information or documents it deems necessary.

3. Notwithstanding a VASP having approval from VARA for the provision of Margin Trading, VARA shall have the power to instruct VASPs to take any of the following actions, in its sole and absolute discretion from time to time, and VASPs must comply with such instructions—
 - a. suspend Margin Trading services for specified Virtual Assets or clients;
 - b. close existing client positions; and
 - c. increase Initial Margin and/or Maintenance Margin requirements.

C. Margin Trading Obligations

1. Without prejudice to any other obligations, VASPs providing Margin Trading services shall—
 - a. obtain information from each client prior to opening a Margin Trading Account to determine whether the Margin Trading service is suitable for a particular client, including but not limited to such information on the client's financial position (including financial solvency), investment objectives, risk appetite, knowledge and experience in trading in Virtual Asset markets as may be relevant and practical;
 - b. ensure that each client's Margin Trading Account is segregated from all other trading accounts;
 - c. only use all Virtual Assets and/or cash balance in the Margin Trading Account as collateral for Margin Trading in accordance with the terms of the Margin Trading Agreement;
 - d. not to utilise the funds of any client to provide the facilities of Margin Trading to another client even if the client's consent has been obtained by the VASP;
 - e. ensure that each client has deposited the Initial Margin in the Margin Trading Account, in accordance with the agreed value, prior to the purchase of any Virtual Assets financed on Margin;
 - f. ensure that, if a client has more than one (1) Margin Trading Account with the VASP, that all risk limits are monitored and maintained at the client level;
 - g. provide each client with a written statement of account at least monthly showing the trading movement of the Virtual Assets financed on Margin and the percentage of their ownership in the Margin Trading Account relative to any Virtual Assets, cash or other assets held as Maintenance Margin;
 - h. monitor on an ongoing basis the Margin Trading Account of each client and provide at least one (1) early warning notification to a client that the percentage of the client's ownership in that account has fallen to a specified percentage and is at risk of falling below the required level of Maintenance Margin specified in the Margin Trading Agreement. The specified percentage at which such early warning notification must be given may be determined by the VASP acting in the best interests of its clients. Such notification must include a full re-statement of the risks required to be stated in the Margin Trading Agreement in Rule IV.E.1.d of this Exchange Services Rulebook below;
 - i. in addition to Rule IV.C.1.h of this Exchange Services Rulebook above, monitor on an ongoing basis the Margin Trading Account of each client and notify the client promptly when the percentage of the client's ownership in that account falls below the required level of Maintenance Margin specified in the Margin Trading Agreement, so that they can cover the shortfall in the account, subject to Rule IV.C.1.j of this Exchange Services Rulebook below;
 - j. in the event that the client is not themselves able to remedy the shortfall within a reasonable timeframe, sell all or some of the Virtual Assets available in the Margin Trading Account to the extent required to restore the client's percentage of ownership to the Maintenance Margin (or such higher level as may be set out in the Margin Trading Agreement) as per the market value of such Virtual Assets on the date of sale;

- k. obtain the prior approval of VARA on any subsequent amendment to the Margin Trading system described in Rule IV.B.2 of this Exchange Services Rulebook above, and provide a technical report confirming that the amended system is able to fulfil the requirements of the Margin Trading service on an ongoing basis, including during times of high volatility; and
- l. ensure that orderly records are kept for the Margin Trading services undertaken for a period of at least eight (8) years.

D. Prudential Requirements, Initial Margin and Maintenance Margin

1. VASPs authorised by VARA to provide Margin Trading services shall—
 - a. ensure that the aggregate funds allocated for Margin Trading services by the VASP are included in the VASPs calculation of its Operational Exposure; and
 - b. ensure that the amount of credit extended to a single client for Margin Trading does not exceed one tenth of the total funds directly or indirectly attributable to Margin Trading by the VASP in its Operational Exposure, in accordance with Rule IV.D.1.a of this Exchange Services Rulebook above.
2. VASPs may only accept the following types of collateral in a Margin Trading Account—
 - a. the Virtual Asset financed on Margin in that account;
 - b. fiat currency; and
 - c. Virtual Asset referencing USD or AED, as approved by VARA.
3. Notwithstanding Rule IV.D.2 of this Exchange Services Rulebook, VASPs may accept the following types of collateral in a Margin Trading Account in the following circumstances—
 - a. other Virtual Assets where there is a continuing fall in the market value of the Virtual Asset financed on Margin; and
 - b. other Virtual Assets where trading in the Virtual Asset financed on Margin is suspended or discontinued for more than seven (7) Working Days or such other period prescribed by VARA.

E. Margin Trading Agreement

1. The Margin Trading Agreement must include the following information—
 - a. an explanation of the VASP's responsibilities and the respective obligations of the VASP and the client including, but not limited to, termination rights, the effect of termination, applicable dispute resolution mechanisms and the VASP's obligation to provide an early warning notification under Rule IV.C.1.h of this Exchange Services Rulebook including when such notifications will be provided;
 - b. whether the client has the right to withdraw cash from the Margin Trading Account, transfer amounts from the Margin Trading Account to the other account, or use such funds for new Margin financing if these amounts are higher than the Maintenance Margin;
 - c. how all financing is calculated, including but not limited to how and when it is paid or payable, the applicable rate, or in the case of a variable rate, how it is calculated and how it may vary and how such variations will be communicated by the VASP to the client;

- d. an explanation of the following risks the client may be exposed to when undertaking Margin Trading, including but not limited to—
 - i. the risk that the client may lose all or part of the funds deposited in the Margin Trading Account;
 - ii. the fact that the VASP may request that the client add Virtual Assets and/or funds in the Margin Trading Account if the Maintenance Margin falls below the prescribed levels or if the VASP increases Maintenance Margin requirements;
 - iii. the right of the VASP to sell all or part of the Virtual Assets in the Margin Trading Account if the Maintenance Margin falls below the percentage specified in the Margin Trading Agreement; and
 - iv. when and how the VASP may sell all or part of the Virtual Assets in the Margin Trading Account;
- e. express consent from the client that they understand, acknowledge and accept each of the risks listed in Rule IV.E.1.d of this Exchange Services Rulebook above;
- f. the applicable levels of Initial Margin and Maintenance Margin and circumstances in which Initial Margin and Maintenance Margin can be amended by the VASP;
- g. a breakdown of the commissions, charges and fees charged by the VASP relating to Margin Trading and when they are payable;
- h. a confirmation of the client's right to pay the cash balance of the price of the remaining Virtual Assets in the Margin Trading Account at any time; and
- i. the fact that in certain situations the position of the client may be liquidated, and that following such liquidation the client may be required to make an additional payment to the VASP.

2. VARA may require any amendments to the Margin Trading Agreement or other forms relating to Margin Trading conducted by a VASP as it deems appropriate.

Schedule 1—Definitions

Term	Definition
“Board”	has the meaning ascribed to it in the Company Rulebook.
“Capital and Prudential Requirements”	has the meaning ascribed to it in the Company Rulebook.
“Client Agreements”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Directive”	has the meaning ascribed to it in the Regulations.
“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to the term ‘Distributed Ledger Technology’ in the Dubai VA Law.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai

	International Financial Centre.
“Entity”	means any legal entity or individual.
“Exchange Services”	has the meaning ascribed to it in Schedule 1 of the Regulations.
“Exchange Services Rulebook”	means this Exchange Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Group”	has the meaning ascribed to it in the Company Rulebook.
“Initial Margin”	<p>means the minimum value of assets which must be deposited by the client in the Margin Trading Account, or otherwise available in the Margin Trading Account but not committed to an existing Margin Trading position, prior to the client opening any new Margin Trading position, which shall be calculated as follows—</p> <p>(a) for Retail Investors—</p> <ul style="list-style-type: none"> i. a minimum of twenty percent (20%) of the notional position value of the new Margin Trading position; or ii. such greater amount as VARA may require for a specific VASP, Virtual Asset or client, from time to time; and <p>(b) for Qualified Investors and Institutional Investors—</p> <ul style="list-style-type: none"> i. such amounts as determined by the VASP's policy; or ii. such greater amount as VARA may require for a specific VASP, Virtual Asset or client, from time to time.
“Institutional Investor”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means holding a valid Licence.
“Maintenance Margin”	means the value of assets which must be deposited by the client in the Margin Trading Account, or otherwise available in the Margin Trading Account but not committed to an existing Margin Trading position, to keep a Margin Trading position open.
“Margin”	means the Initial Margin and any Maintenance Margin provided by a client.
“Margin Trading”	means the financing made by a VASP of a proportion or multiple of the market value of the Virtual Assets financed on margin, and secured as collateral by the Virtual Assets available in the Margin Trading Account or any other collateral in the cases exclusively stated in these Rules.
“Margin Trading Account”	means a type of client account with the VASP, through which dealings in Virtual Assets financed on Margin are executed.
“Margin Trading Agreement”	means the agreement between the VASP and the client specifying the terms and conditions governing the relationship between them in relation to Margin Trading.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Market Offences”	has the meaning ascribed to it in the Regulations.
“Operational Exposure”	has the meaning ascribed to it in the Regulations.

“Paid-Up Capital”	has the meaning ascribed to it in the Company Rulebook.
“Qualified Investor”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Retail Investor”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended VARA from time to time.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity authorised by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.
“Working Day”	has the meaning ascribed to it in the Regulations.

Lending and Borrowing Services Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“**VARA**”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This Lending and Borrowing Services Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out Lending and Borrowing Services in the Emirate.

This Lending and Borrowing Services Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out Lending and Borrowing Services must also comply with the following Rulebooks applicable to all VASPs—

1. Company Rulebook;
2. Compliance and Risk Management Rulebook;
3. Technology and Information Rulebook;
4. Market Conduct Rulebook; and
5. All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

For the avoidance of doubt, where a VASP is Licensed by VARA to carry out other VA Activities in the Emirate in addition to Lending and Borrowing Services, it must comply with all Rulebooks which apply

to those other VA Activities. Unless otherwise stated, the Rules in VA Activity specific Rulebooks apply cumulatively for each VA Activity a VASP carries out.

Capitalised terms in this Lending and Borrowing Services Rulebook have the meanings ascribed to them in the Regulations or as otherwise provided in Schedule 1.

Part I – Policies, Procedures and Public Disclosures

A. Policies and Procedures

1. In addition to all other requirements in the Regulations and Rulebooks, VASPs providing Lending and Borrowing Services shall establish, implement and enforce appropriate written internal policies and procedures relating to the following—
 - a. the ability of clients to have access to and withdraw their Virtual Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility; and
 - b. such other policies and procedures as VARA may require from time to time.
2. VASPs providing Lending and Borrowing Services shall assess and, in any case, at least yearly review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.

B. Public Disclosures

1. VASPs providing Lending and Borrowing Services shall publish on their website in a prominent place or make available by other publicly accessible means—
 - a. a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed;
 - b. their policies and procedures relating to data privacy, whistleblowing and handling of client complaints;
 - c. a statement as to the ability of clients to have access to and withdraw their Virtual Assets, particularly in times of extreme volatility;
 - d. a statement as to the VASP's arrangements for the protection of clients' assets held by the VASP and how it determines uses of client Virtual Assets, including but not limited to a detailed description of such uses;
 - e. a statement as to how they protect client Virtual Assets from counterparty risk, including but not limited to whether the VASP only enters into over-collateralised loans;
 - f. a statement as to how in the course of the provision of Lending and Borrowing Services, client Virtual Assets are used and how clients' interests in respect of those Virtual Assets are thereby respected;
 - g. a statement explaining that client Virtual Assets used by the VASP in the course of the provision of Lending and Borrowing Services may be at risk, including the types and nature of such risks, and a statement on the likelihood and severity of any losses which may be suffered;
 - h. a statement as to how liquidity risk is managed; and
 - i. such other information as VARA may require from time to time.

2. Other disclosable matters. To the extent permissible under applicable laws, VASPs providing Lending and Borrowing Services shall publish on their website or by other publicly accessible means—
 - a. details of any past convictions or prosecutions of any member(s) of their Senior Management or Board, whether before the courts of the UAE or the courts of another jurisdiction; and
 - b. any such other information relating to their business or activities as VARA may reasonably require.
3. The disclosure requirements set out in this Rule I.B of the Lending and Borrowing Services Rulebook are in addition to all disclosures required under the Market Conduct Rulebook and to all notifications to VARA required under the Compliance and Risk Management Rulebook.

C. Activity-Specific Disclosures

1. Interest payments to clients. VASPs providing Lending and Borrowing Services shall, at a minimum, clearly disclose the following in relation to Virtual Assets they borrow from clients—
 - a. the denomination of interest payments (e.g. the type of Virtual Assets) and whether the client has an option to select such denomination and modify the selection at any time;
 - b. the amount and nature (e.g. whether it is a fixed rate or a variable rate) of interest offered to clients in the form of annual percentage yield denominated in the type of borrowed Virtual Asset;
 - c. whether the amount of interest disclosed in Rule I.C.1 of this Lending and Borrowing Services Rulebook is an estimation and if so, provide a description of how such estimation is made by the VASP;
 - d. the frequency at which interest accrues and is credited to client accounts; and
 - e. whether interest is accrued on a simple or compound basis and, if the VASP adopts a tiered approach which offers compound interest for a maximum value of Virtual Assets, the details of such tiered approach.

D. Other Disclosures

1. Lending and Borrowing Services explanation. VASPs shall publish a prominent explanation of—
 - a. their Lending and Borrowing Services;
 - b. specification of which Lending and Borrowing Services are available to which client types; and
 - c. any licensing and regulatory restrictions on Lending and Borrowing Services available to different client types.
2. Lending and borrowing asset and liability report. VASPs shall publish and update at least every three (3) months a lending and borrowing asset and liability report, including but not limited to values of Virtual Assets held, lent or borrowed, pledged or posted as collateral, and how they are held.
3. Governance controls. VASPs providing Lending and Borrowing Services shall publish a clear and transparent explanation of all governance arrangements in respect of—

- a. protocol governance structures to the extent relevant and applicable to the provision of Lending and Borrowing Services, and the loaning and pledging of Virtual Assets to and by clients, as applicable, including client risks in respect of the same; and
- b. whether or not the VASP uses any proprietary protocols in the course of the provision of the Lending and Borrowing Services.

4. Third parties. To the extent that a VASP's Lending and Borrowing Services are made available through, or information communicated via, a third party, the VASP shall also procure that all disclosures and information required by this Part I of the Lending and Borrowing Services Rulebook is provided in an easily accessible location on the website of that third party, in plain and transparent language, in a machine-readable format, and is kept accurate and up-to-date at all times.

Part II – Lending and Borrowing Services Rules

A. General Requirements

1. Liquidity. VASPs providing Lending and Borrowing Services shall, at all times, ensure that—
 - a. they have sufficient Virtual Assets to provide services and satisfy client obligations; and
 - b. sufficient collateral has been posted by borrowers in accordance with agreed amounts, and that both are monitored and audited on a regular basis.
2. VASPs providing Lending and Borrowing Services shall notify VARA immediately if the requirements in Rule II.A.1 of this Lending and Borrowing Services Rulebook are not met, or may not be materially met in the foreseeable future.
3. Withdrawals. VASPs providing Lending and Borrowing Services shall ensure all clients are fully aware when Virtual Assets are not able to be withdrawn as part of the Lending and Borrowing Services they provide. To the extent Virtual Assets are able to be withdrawn, VASPs shall ensure all clients can withdraw such Virtual Assets at all times, and complete withdrawal requests so that Virtual Assets which are the subject of such requests are transferred in accordance with client instructions within twenty-four (24) hours, subject to any factors outside of the VASP's control including limitations or malfunctioning of any DLT not controlled by the VASP or its Group.
4. Collateral. All Virtual Assets held by a VASP providing Lending and Borrowing Services may only be used in accordance with the terms of its Lending and Borrowing Services which, in addition to the requirements in Rule II.E of this Lending and Borrowing Services Rulebook, shall be clearly set out in its Client Agreements. VASPs providing Lending and Borrowing Services shall ensure that they have adequate governance frameworks, policies, systems and controls in place to manage how collateral is held and that it is used responsibly, including in line with Client Agreements at all times.
5. Virtual Assets of a client used by a VASP in the course of, or in connection with, the provision of any Lending and Borrowing Services shall be held on behalf of the client, unless the Client Agreement expressly states otherwise.
6. Counterparty due diligence. VASPs providing Lending and Borrowing Services shall, on a regular basis, conduct comprehensive due diligence on all clients and counterparties such that they are satisfied that client Virtual Assets are not subject to undue counterparty risk. In particular, VASPs shall collect and verify the following information of each counterparty—
 - a. the purpose(s) of loans;
 - b. the nature and type of business;

- c. financial situation and overall liquidity; and
- d. all other information which a prudent lender would require to assess risks associated with a particular loan.

B. Client Reporting & Valuation

1. VASPs providing Lending and Borrowing Services shall, at least monthly, provide to clients a written statement containing the following information—
 - a. the total value of Virtual Assets in a client's account;
 - b. all lending and borrowing transactions entered into between the VASP and the client in the reporting period;
 - c. the amount of interest accrued from and credited to the client's account for lending transactions (both total and during the reporting period);
 - d. the amount of interest paid and debited from the client's account for borrowing transactions (both total and during the reporting period); and
 - e. the amount of collateral posted by the client for borrowing transactions in the reporting period (both total and during the reporting period).
2. VASPs shall maintain accurate and reliable records that are sufficient to confirm and identify all client positions.
3. VASPs providing Lending and Borrowing Services shall ensure that all client positions are subject to independent valuation and client reporting.
4. VASPs shall have comprehensive and well documented valuation policies and procedures in place to ensure the production of timely and accurate valuations in accordance with Rule II.B.1 of this Lending and Borrowing Services Rulebook.

C. Additional Record-Keeping Requirements

1. VASPs providing Lending and Borrowing Services shall maintain the following for at least eight (8) years—
 - a. records of all transactions in relation to their Lending and Borrowing Services, including but not limited to all Client Agreements, agreements with other counterparties and client instructions; and
 - b. information collected from counterparties in accordance with Rule II.A.6 of this Lending and Borrowing Services Rulebook.
2. All records maintained in accordance with Rule II.C.1 of this Lending and Borrowing Services Rulebook must be immediately provided for VARA inspection upon request.

D. Risk Management and Due Diligence

1. Before providing any Lending and Borrowing Services to a client, a VASP shall carry out sufficient due diligence to satisfy itself—

- a. as to the risk profile of such client and transaction at that time and during the course of the Lending and Borrowing Services;
- b. as to the need for, and the suitability of, any collateral to be provided by the client; and
- c. that any collateral is capable of being pledged including under all applicable laws.

2. Before providing any Lending and Borrowing Services on behalf of a third party, VASPs shall ensure that sufficient steps are taken on behalf of such third party to meet the requirements set out in Rule II.D.1 of this Lending and Borrowing Services Rulebook.
3. VASPs shall ensure that liquidity risk and market risk are each monitored and tested regularly, and appropriate measures are put in place as required to address any such risk in a prompt manner.
4. VASPs shall ensure that, to the extent that collateral, including Virtual Assets, is held by them, such collateral is adequate and appropriately protects the VASP against applicable risks. VASPs shall monitor any such risk and record the assessment of such risk regularly and on an ongoing basis. VASPs shall put appropriate measures in place as required to address any such risk in a prompt manner.
5. All such risk management and due diligence must be regularly audited by an independent third party.

E. Client Agreements

1. In addition to all requirements in the Market Conduct Rulebook, Client Agreements for Lending and Borrowing Services shall set out the following, to the extent applicable—
 - a. descriptions of the Virtual Assets lent, borrowed, and/or used as collateral that are sufficient to identify such Virtual Assets;
 - b. any loan-to-value ratio(s) applicable under the Client Agreement;
 - c. the respective rights of the VASP, the client and any other Entity involved in the Lending and Borrowing Services in respect of Virtual Assets that are the subject of the Client Agreement, including in respect of collateral;
 - d. how and when any interest is paid or payable, the applicable rate, or in the case of a variable rate, how it is calculated and how interest may vary, and how such variations will be communicated by the VASP to the client;
 - e. how and when any Virtual Assets lent or borrowed, or held as collateral, are to be held and returned;
 - f. whether or not Virtual Assets of a client used by a VASP in the course of, or in connection with, carrying out any Lending and Borrowing Services, shall be held on behalf of the client;
 - g. any right of the client to withdraw any Virtual Assets lent or borrowed or held as collateral;
 - h. a statement explaining that client Virtual Assets used by the VASP in the course of the provision of Lending and Borrowing Services may be at risk, including the types and nature of such risks, and a statement on the likelihood and severity of any losses which may be suffered;
 - i. any rights of the VASP to vary the terms of the Client Agreement;
 - j. any rights of the VASP and the client to terminate the Client Agreement and the consequences of termination;
 - k. any terms relating to any fluctuation in value of the Virtual Assets to which the Client Agreement relates;
 - l. consequences of any event of default;
 - m. an explanation of the risks the client may be exposed to;

- n. full details of the VASP's client complaints procedure to enable clients to register complaints, as required in relation to the VASP or the services provided by the VASP; and
- o. any requirements necessary for compliance with the governing law of the Client Agreement.

2. In addition to all requirements in the Market Conduct Rulebook, Client Agreements for Lending and Borrowing Services shall obtain the consent of all clients to the use by the VASP of any Virtual Assets of such clients by the VASP (as applicable), in the course of the provision of Lending and Borrowing Services by the VASP. Such consent must be clearly and transparently obtained in accordance with all applicable laws.

Schedule 1 – Definitions

Term	Definition
“Board”	has the meaning ascribed to it in the Company Rulebook.
“Client Agreements”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to the term “Distributed Ledger Technology” in the Dubai VA Law.
“Dubai VA Law”	means <i>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</i> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Lending and Borrowing Services”	has the meaning ascribed to it in <i>Schedule 1</i> of the Regulations.
“Lending and Borrowing Services Rulebook”	means this Lending and Borrowing Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Regulations”	means the <i>Virtual Assets and Related Activities Regulations 2023</i> , as may be amended from time to time.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <i>Schedule 1</i> of the Regulations, as may be amended from time to time.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.

“VASP”	means an Entity authorised by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.

VA Management and Investment Services Rulebook

VA Transfer and Settlement Services Rulebook

Introduction

The Dubai Virtual Assets Regulatory Authority (“VARA”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”), including to issue authorisations to conduct regulated Virtual Asset Activities (“**VA Activities**”).

This VA Transfer and Settlement Services Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out VA Transfer and Settlement Services in and/or from the Emirate.

This VA Transfer and Settlement Services Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out VA Transfer and Settlement Services must also comply with the following Rulebooks applicable to all VASPs—

1. Company Rulebook;
2. Compliance and Risk Management Rulebook;
3. Technology and Information Rulebook;
4. Market Conduct Rulebook; and
5. All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

For the avoidance of doubt, where a VASP is Licensed by VARA to carry out other VA Activities in the Emirate in addition to VA Transfer and Settlement Services, it must comply with all Rulebooks that apply to those other VA Activities. Unless otherwise stated, the Rules in VA Activity specific Rulebooks apply cumulatively for each VA Activity a VASP carries out.

Capitalised terms in this VA Transfer and Settlement Services Rulebook have the meanings ascribed to them in the Regulations or as otherwise provided in Schedule 1.

Introduction

The Dubai Virtual Assets Regulatory Authority (“VARA”) was established and authorised by Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai (“**Dubai VA Law**”) to regulate Virtual Asset Service Providers (“**VASPs**”).

This VA Management and Investment Services Rulebook is issued pursuant to, and forms part of, the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), issued by VARA, and applies to all VASPs Licensed by VARA to carry out VA

Management and Investment Services in the Emirate.

This VA Management and Investment Services Rulebook applies in addition to all other requirements in the Regulations as may be in force from time to time. As such, VASPs Licensed by VARA to carry out VA Management and Investment Services must also comply with the following Rulebooks applicable to all VASPs—

1. Company Rulebook;
2. Compliance and Risk Management Rulebook;
3. Technology and Information Rulebook;
4. Market Conduct Rulebook; and
5. All Rulebooks specific to the VA Activities that a VASP is Licensed by VARA to carry out.

For the avoidance of doubt, where a VASP is Licensed by VARA to carry out other VA Activities in the Emirate in addition to VA Management and Investment Services, it must comply with all Rulebooks which apply to those other VA Activities. Unless otherwise stated, the Rules in VA Activity specific Rulebooks apply cumulatively for each VA Activity a VASP carries out.

Capitalised terms in this VA Management and Investment Services Rulebook have the meanings ascribed to them in the Regulations or as otherwise provided in Schedule 1.

Part I – Policies, Procedures and Public Disclosures

Part I – Policies, Procedures and Public Disclosures

A. Policies and Procedures

1. In addition to all other requirements in the Regulations and Rulebooks, VASPs providing VA Management and Investment Services shall establish, implement and enforce appropriate written internal policies and procedures relating to the following—
 - a. the ability of clients to have access to and withdraw their Virtual Assets including, but not limited to, during periods of high uncertainty and/or extreme volatility;
 - b. their assessment of client suitability for relevant products or services, including but not limited to the nature, features, costs and risks of investment services, Virtual Assets or other financial instruments selected for their clients, while taking into account cost and complexity;
 - c. how they ensure all Staff providing VA Management and Investment Services to clients are sufficiently competent in accordance with Rule II.B.1 of this VA Management and Investment Services Rulebook; and
 - d. such other policies and procedures as VARA may require from time to time.
2. VASPs providing VA Management and Investment Services shall assess and, in any case, at least yearly review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.

A Policies and Procedures

1. In addition to all other requirements in the Regulations and Rulebooks, VASPs providing VA Transfer and Settlement Services shall establish, implement and enforce appropriate written internal policies and procedures relating to the following—
 - a. how they will rectify any non-executed, defectively executed or incomplete Virtual Assets transmission, transfer and/or settlement in the course of providing VA Transfer and Settlement Services, including but not limited to refunding affected clients;
 - b. the Default Rules as prescribed in Rule II.H of this VA Transfer and Settlement Services Rulebook, below; and
 - c. such other policies or procedures as VARA may require from time to time.
2. VASPs providing VA Transfer and Settlement Services shall assess and, in any case at least yearly, review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.

B Public Disclosures

1. VASPs providing VA Transfer and Settlement Services shall publish on their website in a prominent place or make available by other publicly accessible means—
 - a. a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed;
 - b. their policies and procedures relating to data privacy, whistleblowing and handling of client complaints;
 - c. a statement of whether the VASP refers or introduces clients to other Entities including, but not limited to, other VASPs and, if so, a description of the terms of such arrangements and the monetary or non-monetary benefits received by the VASP, including by way of reciprocation for any service or business; and
 - d. a statement of whether the VASP has accounts, funds or Virtual Assets maintained by a third party and if so, provide the identity of that third party; and
 - e. such other information as VARA may require from time to time.
2. Other disclosable matters. To the extent permissible under applicable laws, VASPs providing VA Transfer and Settlement Services shall publish on their website, or by other publicly accessible means—
 - a. details of any past convictions or prosecutions of any member(s) of their Senior Management or Board, whether before the courts of the UAE or the courts of another jurisdiction; and
 - b. any such other information relating to their business or activities as VARA may reasonably require.
3. The disclosure requirements set out in this Rule I.B of the VA Transfer and Settlement Services Rulebook are in addition to all disclosures required under the Market Conduct Rulebook, and to all notifications to VARA required under the Compliance and Risk Management Rulebook.

B. Public Disclosures

1. VASPs providing VA Management and Investment Services shall publish on their website in a prominent place or make available by other publicly accessible means—
 - a. a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed;
 - b. their policies and procedures relating to data privacy, whistleblowing and handling of client complaints;
 - c. a statement as to the ability of clients to have access to and withdraw their Virtual Assets, particularly in times of extreme volatility;
 - d. a statement as to the VASP's arrangements for the protection of clients' assets held by the VASP and how it determines uses of client Virtual Assets including but not limited to a detailed description of such uses;
 - e. a statement as to how they protect client Virtual Assets from counterparty risk;
 - f. a statement as to how in the course of the provision on VA Management and Investment Services, client Virtual Assets are used and how clients' interests in respect of those Virtual Assets are thereby respected;
 - g. a statement explaining that client Virtual Assets used by the VASP in the course of the provision of VA Management and Investment Services may be at risk, including the types and nature of such risks, and a statement on the likelihood and severity of any losses which may be suffered;
 - h. a statement in relation to order execution by the VASP;
 - i. a statement as to how liquidity risk is managed; and
 - j. such other information as VARA may require from time to time.
2. Other disclosable matters. To the extent permissible under applicable laws, VASPs providing VA Management and Investment Services shall publish on their website or by other publicly accessible means—
 - a. details of any past convictions or prosecutions of any member(s) of their Senior Management or Board, whether before the courts of the UAE or the courts of another jurisdiction; and
 - b. any such other information relating to their business or activities as VARA may reasonably require.
3. The disclosure requirements set out in this Rule I.B of this VA Management and Investment Services Rulebook are in addition to all disclosures required under the Market Conduct Rulebook and to all notifications to VARA required under the Compliance and Risk Management Rulebook.

Part II – VA Management and Investment Services Rules

Part II – VA Transfer and Settlement Rules

A. General Requirements

1. In addition to the Rules in this Part II of the VA Transfer and Settlement Services Rulebook, VASPs providing VA Transfer and Settlement Services must also comply with all applicable legal and regulatory requirements issued by the CBUAE which apply to the VASP including, but not limited to, all such applicable legal and regulatory requirements, which pertain to the end-to-end

enablement of payments, remittances and/or other related services as may be amended from time to time.

2. In addition to the Rules in this Part II of the VA Transfer and Settlement Services Rulebook, VASPs providing VA Transfer and Settlement Services must ensure that they comply with all legal and regulatory requirements for such services, inside and outside of the UAE. VASPs must ensure at all times that any transmission, transfer and/or settlement being undertaken is permissible and can be facilitated through, and concluded in, all jurisdictions that are relevant to that transmission, transfer and/or settlement.
3. In addition to all other requirements in the Compliance and Risk Management Rulebook, VASPs providing VA Transfer and Settlement Services must comply with all requirements with respect to AML/CFT contained in that Rulebook, including but not limited to FATF-specific compliance requirements such as the Travel Rule.

A. Client Suitability

1. VASPs providing VA Management and Investment Services shall only provide such services regarding Virtual Assets to clients for which they are suitable.
2. Where VASPs provide VA Management and Investment Services which include a personal recommendation to a client, they shall consider the following factors at a minimum in respect of that client—
 - a. knowledge and experience in investing in Virtual Assets;
 - b. investment objectives, including but not limited to risk tolerance, time horizon and venues through which they can acquire Virtual Assets; and
 - c. financial circumstances including, but not limited to, their ability to bear sudden and significant losses or the proportion of their net worth which is invested in Virtual Assets.
3. VASPs providing VA Management and Investment Services shall collect all necessary information from clients for the purpose of assessing relevant factors in accordance with Rules II.A.1 and II.A.2 of this VA Management and Investment Services Rulebook, depending on the nature of the service and take all reasonable steps to ensure such information is accurate and up-to-date. All such information shall be maintained for at least eight (8) years.
4. To the extent Rule II.A.2 of this VA Management and Investment Services Rulebook is applicable, VASPs shall specify how the services are appropriate for a client by reference to the factors assessed by the VASP in accordance with Rule II.A.2 of this VA Management and Investment Services Rulebook.

B. Staff Competency

1. In addition to all requirements in the Company Rulebook, VASPs providing VA Management and Investment Services shall ensure all of their Staff are knowledgeable, competent and suitably trained given the nature of their role. In assessing Staff competency, VASPs shall consider the following factors at a minimum in the context of the role of the Staff member concerned—
 - a. academic, professional and industry qualifications;
 - b. experience in the Virtual Assets sector, including but not limited to hands-on working experience acquired through their employment by Entities carrying out activities similar to VA Activities outside of the Emirate;

- c. whether they have a good understanding of the VARA regulatory framework, including but not limited to the Regulations, Rules and Directives governing the provision of VA Management and Investment Services; and
- d. industry standards as may be applicable to the Virtual Assets sector from time to time.

B. Property Interests and Protection of Client Virtual Assets

1. VASPs providing VA Transfer and Settlement Services are prohibited from selling, transferring, assigning, lending, rehypothecating, pledging, converting into another Virtual Asset, or otherwise using or encumbering any Virtual Assets for the purposes of a transmission, transfer and/or settlement, or authorising or permitting the same, except when authorised by explicit consent from their client to do so, as part of the VA Transfer and Settlement Services being provided to that client.
2. The consent required under Rule II.B.1 of this VA Transfer and Settlement Services Rulebook must be secured through explicit instruction from, or acceptance by the client prior to the VASP carrying out any VA Transfer and Settlement Services for that client, but is not required on a per transmission, transfer and/or settlement basis, unless explicitly required by the client, insofar as the said transmission, transfer and/or settlement meets the conditions consented to by the client.

C. Verification of Information

1. VASPs providing VA Management and Investment Services shall not provide statements, promises, forecasts or other types of information which they know or suspect to be misleading, false or deceptive or which they should have reasonably known to be misleading, false or deceptive at the time of making such statement, promise or forecast.
2. Prior to making any statement, promise or forecast, VASPs providing VA Management and Investment Services shall verify factual information against appropriate and reliable source materials and shall use all reasonable endeavours to verify the continued accuracy of such information.

C. Authorisation and Responsibility for Transmissions, Transfers and/or Settlements

1. VASPs must have procedures for ensuring that all VA Transfer and Settlement Services carried out for a client are authorised by the relevant client, and that the VASP is acting in accordance with the client's instructions at all times.
2. To the extent that any Virtual Assets transmission, transfer and/or settlement processed by a VASP as part of any VA Transfer and Settlement Services is not authorised by the relevant client, or is not carried out by the VASP in accordance with the client's instructions due to any reason whether or not it is a VASP triggered consequence, the VASP—
 - a. shall, as soon as practicable but in all events within twenty-four (24) hours of becoming aware of such erroneous execution, refund the client or otherwise restore the client's account to the state it would have been in, had the wrongful transmission, transfer and/or settlement not been effected; and
 - b. is liable to the client in respect of the loss suffered by the client as a direct result of the VASP's actions or omissions.

3. Where a VASP's client is the sender of a Virtual Assets transmission, transfer and/or settlement, the VASP is liable to its client for the correct transmission, transfer and/or settlement of the Virtual Assets to the recipient, whether the transmission, transfer and/or settlement is to the recipient's VASP (if applicable) or VA Wallet. To the extent that any such Virtual Assets transmission, transfer and/or settlement is not received by the target recipient, the VASP must make immediate efforts to trace the Virtual Assets, establish the cause of the failure, and notify its client (the sender) of the outcome. The VASP shall only be deemed to have fulfilled its responsibility if and when it is able to prove that it is not liable in respect of a non-executed, defectively executed or incomplete Virtual Assets transmission, transfer and/or settlement.
4. A recipient's VASP (if applicable) is responsible for the systemic readiness and infrastructural functioning of VA Wallets and/or accounts of its clients for the purposes of receiving Virtual Assets, as well as providing all routing information that is necessary for a transmission, transfer and/or settlement to be completed when requested by the sender's VASP. To the extent that any Virtual Assets transmission, transfer and/or settlement is not received by the target recipient, the recipient VASP shall only be liable if and when the sender's VASP can establish that it has executed the transmission, transfer and/or settlement in accordance with the instructions, and that the error was caused by the recipient's VASP.
5. VASPs must maintain records of all client instructions for a period of eight (8) years.

D. Impermissible Activities

1. VASPs shall not authorise or permit rehypothecation of Virtual Assets for which they provide VA Management and Investment Services unless they have explicit prior consent from the client to do so.
2. VASPs providing VA Management and Investment Services shall only use or exercise authority relating to a Virtual Asset based on valid authorisation and/or specific instructions from the client.
3. Virtual Assets of a client used by a VASP in the course of, or in connection with, the provision of any VA Management and Investment Services shall be held on behalf of the client unless the Client Agreement expressly states otherwise.

D. Client Disclosures

1. In addition to all requirements in the Market Conduct Rulebook, prior to entering into any Client Agreements to provide VA Transfer and Settlement Services, VASPs must disclose to clients and potential clients all material risks associated with using Virtual Assets in connection with the VA Transfer and Settlement Services, including but not limited to—
 - a. Virtual Assets transactions may be irreversible, meaning that any losses suffered because of fraud or an accidental or unauthorised transaction may not be recoverable;
 - b. Virtual Assets transactions may not be finalised until recorded on the relevant DLT for the Virtual Asset, which may not be the time or date that the client initiates the transmission, transfer and/or settlement; and
 - c. Virtual Assets may experience technical difficulties unrelated to actions by the VASP that may in turn impact the client's ability to access or use the Virtual Assets for transmissions, transfers and/or settlements.
2. In addition to all requirements in the Market Conduct Rulebook, prior to entering into any Client Agreements to provide VA Transfer and Settlement Services, VASPs must disclose all the relevant terms and conditions associated with the VA Transfer and Settlement Services,

including, as applicable, the following—

- a. a fee schedule listing—
 - i. all fees and charges and how they will be paid;
 - ii. how the fees and charges are calculated, if they are not set in advance; and
 - iii. when they will be assessed;
- b. information about execution times;
- c. whether the client has a right to stop or amend a pre-authorised transmission, transfer and/or settlement, or revoke authorisation for a transmission, transfer and/or settlement, including the required procedure to initiate stop-settlement orders, or revoke the authorisation for a subsequent transmission, transfer and/or settlement;
- d. the client's and the VASP's respective liabilities for any unauthorised, mistaken, or accidental transmission, transfer and/or settlement;
- e. general error-resolution rights that apply to transmission, transfer and/or settlement;
- f. the client's right to receive periodic account statements and Virtual Asset valuations from the VASP;
- g. the client's right to receive a receipt or other evidence of a Virtual Asset transmission, transfer and/or settlement; and
- h. to the extent relevant—
 - i. any ability of the VASP to vary unilaterally the terms of any contract with the client for the provision of VA Transfer and Settlement Services, and client's right to terminate such contract. If the client is a Retail Investor, terms and conditions shall specify—
 1. that any notice to vary unilaterally shall be provided by the VASP to the client no later than sixty (60) calendar days before the date on which any change is due to take effect; and
 2. that the client must have a right to terminate the contract without charge at any time before such a change takes effect, which the VASP shall also communicate at the time of giving notice.

In respect of any other type of client, the VASP and the client may agree to waive such requirements; and

 - ii. any ability of the VASP and/or client to terminate a contract for the provisions of VA Transfer and Settlement Services. If the client is a Retail Investor, the terms and conditions shall—
 1. specify that the client may terminate the contract at any time unless the client and the VASP have agreed a notice period of no more than thirty (30) calendar days; and
 2. that the VASP may terminate a contract by giving at least sixty (60) calendar days' notice.
3. VASPs providing VA Transfer and Settlement Services may not exclude, or attempt to exclude, any form of actual or potential liability in respect of the VA Transfer and Settlement Services by virtue of having provided the disclosures required under this Rule II.D of the VA Transfer and Settlement Services Rulebook.

E. Exchange, Trade or Conversion

1. In addition to all other requirements in this VA Transfer and Settlement Services Rulebook, VASPs providing VA Transfer and Settlement Services which involve any exchange, trade or conversion between the Virtual Assets received and another Virtual Asset or fiat currency, must—
 - a. use a VASP Licensed by VARA for Exchange Services or, if using an Entity outside of the Emirate, as approved by VARA;
 - b. continue to act honestly, fairly and in good faith;
 - c. provide a description of how they undertake any exchange, trade or conversion to their clients or potential clients, including whether they use any third party, and the nature of the role of such third party;
 - d. disclose all relevant terms and conditions associated with the exchange, trade or conversion to their clients or potential clients, including but not limited to applicable fees;
 - e. do everything within their control to ensure completion of the transmission, transfer and/or settlement thereafter, including any such exchange, trade or conversion, subject only to limitations or malfunctioning of any DLT in the event they are not controlled directly or indirectly by the VASP or its Group; and
 - f. remain directly responsible to their clients for the completion of the transmission, transfer and/or settlement as relevant.

E. Client Reporting & Valuation

1. VASPs providing VA Management and Investment Services shall, at least monthly, provide to each client a written statement containing the following information—
 - a. the total value of Virtual Assets in a client's account;
 - b. all transactions entered into between the VASP and the client in the reporting period; and
 - c. the change in amount and valuation of Virtual Assets in a client's account (both total and during the reporting period).
2. VASPs providing VA Management and Investment Services shall ensure that all assets under management are subject to ongoing independent valuation.
3. VASPs shall have comprehensive and well documented valuation policies and procedures in place to ensure the production of timely and accurate valuation in accordance with Rule II.E.1 of this VA Management and Investment Services Rulebook.

F. Receipts

1. Immediately after receiving client instructions to initiate a transmission, transfer and/or settlement, a VASP must provide the client with a receipt including the following information—
 - a. confirmation of whether the transmission, transfer and/or settlement has been successfully initiated;
 - b. date and time of receipt of the client's instructions;
 - c. amount and type of Virtual Assets in the transmission, transfer and/or settlement;

- d. name and unique identifier of the Entity to which transmission, transfer and/or settlement is to be credited;
- e. name of the client who made the transmission, transfer and/or settlement;
- f. a breakdown of all fees paid or payable by the client and when they are paid or payable;
- g. a breakdown of all exchanges, trades or conversions to be completed in the course of any transmission, transfer and/or settlement (if applicable);
- h. transaction identification details and/or reference;
- i. the VASP's name and contact information, including information necessary for the client to ask a question or file a complaint;
- j. a statement regarding the VASP's liability for non-delivery or delayed delivery; and
- k. a statement regarding the VASP's refund policy.

2. Immediately after a transmission, transfer and/or settlement has been finalised, a VASP must provide the client with a receipt including the following information—

- a. date and time of the transmission, transfer and/or settlement being credited to the recipient;
- b. amount and type of Virtual Assets in the transmission, transfer and/or settlement;
- c. transaction identification details and/or reference; and
- d. full details of all exchanges, trades or conversions completed in the course of the transmission, transfer and/or settlement (if applicable), including times, rates of exchange and all fees.

3. VASPs must maintain all receipts provided in accordance with Rules II.F.1 and II.F.2 of this VA Transfer and Settlement Services Rulebook for a period of eight (8) years.

F. Fees and Charges

1. No payment may be made, or benefit given, to the VASP out of any Virtual Assets under its management, whether by way of fees for its services, reimbursement of expenses or otherwise, unless it is permitted by the Client Agreement and the Client Agreement specifies how it will be calculated and accrued, and when it will be paid.
2. VASPs must not introduce a new category of fees for their services or make any increase in the current rate or amount of its fees payable out of any Virtual Assets under its management unless the VASP has given not less than ninety (90) calendar days' written notice of that introduction or increase and of the date of its commencement to its clients.

G. Benchmark Global Standards

1. VASPs providing VA Transfer and Settlement Services must be able to demonstrate alignment on relevant internationally accepted standards for financial market infrastructures, to VARA's satisfaction.
2. VASPs providing VA Transfer and Settlement Services must ensure that such services include satisfactory arrangements for securing the timely discharge of the obligations in the context of transactions for which it provides such services.
3. In complying with Rule II.G.1 above, VASPs providing VA Transfer and Settlement Services should have regard to their—

- a. practices relating to settlement including, but not limited to, the conditions agreed with clients for the provision of VA Transfer and Settlement Services;
- b. where relevant, arrangements for matching transfers and/or trades and ensuring that the parties are in agreement about such transfers and/or trade details;
- c. where relevant, arrangements for making deliveries and payments in all relevant jurisdictions;
- d. notwithstanding Rule II.H below, procedures to detect and deal with the failure of a client to settle in accordance with the conditions agreed;
- e. arrangements for taking action to settle a transfer and/or trade if a client does not settle, in accordance with the conditions agreed; and
- f. arrangements for monitoring its clients' settlement performance.

G. Marketing

- 1. VASPs providing VA Management and Investment Services shall not represent in any Marketing that their services involve the distribution of 'staking' rewards in relation to any DLT with a 'proof-of-stake' consensus mechanism or any other similar protocol-based rewards to clients, unless the payments actually made to clients by the VASP directly originate from such 'staking' rewards or other similar protocol-based rewards.

H. Management Practices

- 1. When providing VA Management and Investment Services in respect of Virtual Assets on behalf of clients, VASPs shall act in the best interests of their clients at all times. Factors that VASPs may consider when assessing a client's best interests may include, but are not limited to, client suitability, the price of Virtual Assets, costs, speed, likelihood of execution and settlement, size, nature, conditions of custody, and such other conditions as are relevant to the management of Virtual Assets, provided that the VASP must act in accordance with any specific instructions provided by the client.

H. Default Rules

- 1. VASPs providing VA Transfer and Settlement Services must have legally enforceable rules in the event of a client being, or appearing to be, unable to meet its obligations in respect of one or more transmission, transfer and/or settlement, which enable action to be taken in respect of the unsettled transmission, transfer and/or settlement to which the client has undertaken obligations or is a party ("Default Rules").
- 2. Such Default Rules must be appropriate, and demonstrate due consideration, for all risks given the nature of transmission, transfer and/or settlement, including but not limited to the following—
 - a. effecting any close-out transfers of a defaulting client's assets or positions (as applicable) to the VASP or a non-defaulting client;
 - b. the application of the proceeds of liquidation and/or other funds and assets of the defaulting client;
 - c. the use of a default contribution fund mechanism pertaining to clients' pre-funded contributions becoming applicable in the event of a default;
 - d. all remaining rights and liabilities of the defaulting client in respect of an unsettled transmission, transfer and/or settlement;

- e. segregation and portability arrangements, including the method for determining the value at which client positions will be transferred;
- f. provisions ensuring that losses that arise as a result of any default do not threaten the solvency of the VASPs providing VA Transfer and Settlement Services, and that the VASP can continue to provide the services and carry out the activities; and
- g. restriction of any further transmission, transfer, trade or termination of a client's access to the VA Transfer and Settlement Services in the event of such client's failure to meet its obligations in respect of one or more transmission, transfer or trade.

3. The Default Rules shall clearly define and specify:

- a. circumstances which constitute a default, addressing both financial and operational default, and how the different types of default may be treated by the VASP providing VA Transfer and Settlement Services;
- b. the method for identifying a default, including any automatic or discretionary default scenarios, and how the discretion is exercised in any relevant default scenarios;
- c. potential changes to the normal settlement practices in a default scenario;
- d. the management of transmissions or transfer at different stages of processing a transmission, transfer and/or settlement;
- e. the treatment of Client Money and/or Client VAs;
- f. the probable sequencing of actions that the VASP providing VA Transfer and Settlement Services will expect to take under the Default Rules;
- g. the roles, obligations and responsibilities of various parties, including the VASP providing VA Transfer and Settlement Services, the defaulting client and non-defaulting clients;
- h. how to contain the chain effect of the defaulting client's obligations and its implications in the wider ecosystem including, but not limited to, other clients of the VASP;
- i. how to address the allocation of any credit losses it may face, as a result of any individual or combined default, and how stress events are dealt with;
- j. any other mechanisms that may be activated to contain the impact of a default, including—
 - i. whether the VASP maintains a default contribution fund, whereby defaulting and non-defaulting clients' or participants' pre-funded contributions are applied to cover the losses or shortfalls resulting from a default on the basis of a predetermined order of priority; and
 - ii. a resolution regime of the defaulting participant, involving 'porting' or transferring the open positions and margin related to client transactions to a non-defaulting participant, receiver, third party or bridge financial company.

4. Default Rules should be reviewed and tested at least annually, or following material changes to the rules and procedures, to ensure that they are practical and effective.

I. Receipt and Transmission of Orders

1. VASPs shall establish and implement procedures and arrangements for the prompt and proper transmission of client's instructions in respect of Virtual Assets for which VA Management and Investment Services are provided.
2. VASPs shall not receive any remuneration, discount or other benefit for routing clients' orders to a particular trading platform or VASP in the course of the provision of VA Management and

Investment Services, unless disclosed in the Client Agreement and the VASP has obtained valid acceptance in accordance with applicable laws.

3. VASPs shall not misuse information relating to clients' Virtual Assets and their management thereof.

J. Risk Management and Due Diligence

1. In addition to all requirements in the Company Rulebook, VASPs shall ensure that liquidity risk and market risk are each monitored and tested regularly, and appropriate measures put in place as required to address any such risk in a prompt manner.
2. All such risk management and due diligence must be regularly audited by an independent third party and provided to VARA upon request.

K. Client Agreements

1. In addition to all requirements in the Market Conduct Rulebook, Client Agreements for VA Management and Investment Services shall set out the following, to the extent applicable—
 - a. description of Virtual Assets in-scope of VA Management and Investment Services that are sufficient to identify them;
 - b. the respective rights of the VASP, the client and any other Entity involved in the VA Management and Investment Services in respect of Virtual Assets that are the subject of the Client Agreement, including in respect of staking;
 - c. how and when any proceeds are paid or payable, or in the case of variable proceeds, how they are calculated, how the proceeds may vary and how such variations will be communicated by the VASP to the client;
 - d. whether or not Virtual Assets of a client used by a VASP in the course of, or in connection with, any VA Management and Investment Services, shall be held on behalf of the client;
 - e. the consent of the client shall be clearly obtained in accordance with all applicable laws for the use of any Virtual Assets used in the course of the provision of VA Management and Investment Services by the VASP;
 - f. any right of the client to withdraw any Virtual Assets held by the VASP;
 - g. a statement explaining that client Virtual Assets used by the VASP in the course of the provision of VA Management and Investment Services may be at risk, including the types and nature of such risks, and a statement on the likelihood and severity of any losses which may be suffered;
 - h. any rights of the VASP to vary the terms of the Client Agreement;
 - i. any rights of the VASP and the client to terminate the Client Agreement and the consequences of termination;
 - j. any terms relating to any fluctuation in value of the Virtual Assets to which the Client Agreement relates;
 - k. consequences of any event of default;
 - l. an explanation of the risks the client may be exposed to;
 - m. full details of the VASP's client complaints procedure; and
 - n. whether the VASP receives any remuneration, discount or other benefit for routing clients' orders to a particular trading platform or VASP in the course of provision of VA Management and Investment Services.

Schedule 1 – Definitions

Term	Definition
“Board”	has the meaning ascribed to it in the Company Rulebook.
“Client Agreements”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Directive”	has the meaning ascribed to it in the Regulations.
“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to the term “Distributed Ledger Technology” in the Dubai VA Law.
“Dubai VA Law”	means <i>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</i> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Marketing”	has the meaning ascribed to it in <i>The Regulations on the Marketing of Virtual Assets and Related Activities 2024</i> .
“Regulations”	means <i>the Virtual Assets and Related Activities Regulations 2023</i> , as may be amended from time to time.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Staff”	has the meaning ascribed to it in the Company Rulebook.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <i>Schedule 1</i> of the Regulations, as may be amended VARA from time to time.
“VA Management and Investment Services”	has the meaning ascribed to it in <i>Schedule 1</i> of the Regulations.
“VA Management and Investment Services Rulebook”	means this VA Management and Investment Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity authorised by VARA to conduct VA Activity(ies) in the Emirate.

“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.
-------------------------	---

Schedule 1 – Definitions

Term	Definition
“AML/CFT”	has the meaning ascribed to it in the Regulations.
“Board”	has the meaning ascribed to it in the Company Rulebook.
“CBUAE”	means the Central Bank of the United Arab Emirates.
“Client Agreements”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Client Money”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Client VA”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Default Rules”	has the meaning ascribed to it in Rule II.H.1 of this VA Transfer and Settlement Services Rulebook.
“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to the term ‘Distributed Ledger Technology’ in the Dubai VA Law.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Group”	has the meaning ascribed to it in the Company Rulebook.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Retail Investor”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“Rulebook”	has the meaning ascribed to it in the Regulations.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Travel Rule”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.

“VA Transfer and Settlement Services”	has the meaning ascribed to it in Schedule 1 of the Regulations.
“VA Transfer and Settlement Services Rulebook”	means this VA Transfer and Settlement Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“VA Wallet”	has the meaning ascribed to the term ‘Virtual Asset Wallet’ in the Dubai VA Law.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VASP”	means an Entity authorised by VARA to conduct VA Activity(ies) in the Emirate.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.

Virtual Asset Issuance Rulebook

Introduction

This Virtual Asset Issuance Rulebook (“**VA Issuance Rulebook**”) is issued by VARA pursuant to the Virtual Assets and Related Activities Regulations 2023, as may be amended from time to time (“**Regulations**”), and includes requirements that all Entities in the Emirate wishing to issue a Virtual Asset must follow.

The requirements defined herein cover explicit categories and conditions to be met for VA issuances in each category, including but not limited to—

- Category 1 VA Issuances that require a VARA Licence;
- Category 2 VA issuances; and
- Exempt VA issuances.

The Rules contained in this VA Issuance Rulebook operate in addition to the regulation of VA Activities carried out in the Emirate.

In order to address emerging risks and the continually evolving developments in the Virtual Assets sector globally and in the Emirate, VARA will continue to monitor these Rules and any Annex hereto and amend them from time to time. In addition to the Rules in this VA Issuance Rulebook, specific Rules or Directives for certain types of Virtual Assets (as defined by VARA) shall be made available from time to time.

The most updated version of the Regulations, this VA Issuance Rulebook and any additional Rules or Directives shall be made available on VARA’s website.

Capitalised terms in this VA Issuance Rulebook have the meanings defined herein or as defined in Schedule 2 – Definitions.

Disclaimer

Any Licence granted by VARA under this VA Issuance Rulebook is not an endorsement of either (i) the Issuer or (ii) any Virtual Asset and must not be construed or considered as such.

A Licence to issue Virtual Assets granted by VARA under this VA Issuance Rulebook does not exempt any Entity from obtaining relevant approvals in respect of any specific Virtual Asset where mandated under any VARA Regulations, Rules or Directives.

Unless otherwise specified in its communications, VARA makes no representation and does not provide any warranties regarding any Issuer or Virtual Asset including, but not limited to, their fitness for purpose, suitability or regulatory status in any jurisdiction other than the Emirate of Dubai, UAE.

Any representation contrary to the above shall be deemed to be a breach of the Virtual Assets and Related Activities Regulations 2023, as amended from time to time.

Part I – Licence Requirements

A. General Requirement

1. All Entities in the Emirate that issue a Virtual Asset in the course of a business, must comply with this VA Issuance Rulebook, as may be amended by VARA from time to time.
2. “In the course of a business” requirement. For the purposes of Rule I.A.1 of this VA Issuance Rulebook, in determining whether an Entity has issued a Virtual Asset in the course of a business, VARA shall retain sole and absolute discretion, with the following factors forming part of the consideration criteria—
 - a. whether the Entity holds itself out as issuing the Virtual Asset in the course of a business;
 - b. the regularity and scale with which the Entity issues Virtual Assets;
 - c. whether there is any direct or indirect commercial element to the Virtual Asset or in how the Virtual Asset is issued;
 - d. whether the Entity receives remuneration, incentive or other value in kind benefit;
 - e. whether the Entity is related to any commercial or business activity in any way;
 - f. includes not-for-profit, non-profit and charitable organisations, foundations, associations and associated activity(ies);
 - g. Category 1 VA Issuances are, in all events without exception, deemed to be carried out in the course of a business; and
 - h. VA issuances that do not fall under Category 1, and that are carried out solely for personal and/or non-commercial use, may not be deemed to be issued in the course of a business.
3. VARA will, from time to time, assign categorisations to the issuance of certain types of Virtual Assets depending on the nature of the issuance and/or underlying business model associated with the Virtual Asset. VARA may impose additional specific or nuanced requirements on such issuances which, unless otherwise stated, will apply in addition to the requirement for the Issuer to obtain a Licence and/or thereafter obtain prior approval from VARA of the Whitepaper.

B. Prohibited Virtual Assets

1. As specified in the Regulations, issuing Anonymity-Enhanced Cryptocurrencies and all VA Activity(ies) related to them are prohibited in the Emirate.

C. VA issuance Categories and Prior Requirements

- VA issuances in the Emirate are categorised, along with the applicable requirement prior to the Virtual Asset being issued, as follows—

Category	Applicable types of VA issuances	Prior requirement
Category 1	issuance of— (i) Fiat-Referenced Virtual Assets (“ FRVAs ”); (ii) Asset-Referenced Virtual Assets (“ ARVAs ”); or (iii) other Virtual Assets as may be determined by VARA from time to time.	VARA Licence.
Category 2	Issuance of any Virtual Asset which does not constitute— (i) a Category 1 VA Issuance; or (ii) an Exempt VA.	No VARA Licence required, but all placement or distribution must be carried out through or by a Licensed Distributor.
Exempt VAs	Issuance of any Virtual Asset which does not constitute a Category 1 VA Issuance and is either— (i) a Non-Transferable Virtual Asset; (ii) a Redeemable Closed-Loop Virtual Asset; or (iii) other Virtual Asset as may be determined by VARA from time to time.	No requirements prior to issuance.

- When determining the category of a VA issuance, VARA will consider all factors it deems appropriate, including but not limited to, the—
 - nature of all Virtual Assets or types of Virtual Assets;
 - rights and/or value which the Virtual Asset represents or purports to represent; and
 - the underlying business model associated with the Virtual Asset.
- If any change is proposed to a Virtual Asset which may result in its issuance no longer qualifying under the original categorisation in Rule I.C.1 of this VA Issuance Rulebook, the Issuer must comply with all requirements of the category under which the Virtual Asset will fall after such change has been made. The Issuer must ensure all such future requirements are met prior to any proposed change to the Virtual Asset taking effect which, for the avoidance of doubt, may include the Issuer obtaining a Licence from VARA and/or thereafter obtaining prior approval from VARA of the Whitepaper, where necessary.

D. Category 1 VA Issuance

- No Entity in the Emirate may carry out any Category 1 VA Issuance, unless it is authorised and Licensed by VARA for the VA issuance.
- As stated in the Regulations, carrying out Category 1 VA Issuance is a VA Activity. In addition to compliance with this VA Issuance Rulebook, and all other Regulations, Rules and Directives as communicated by VARA in its Licence, or otherwise from time to time, all Entities seeking to carry out Category 1 VA Issuance will be required to comply with the following Rulebooks—

- a. Company Rulebook;
- b. Compliance and Risk Management Rulebook;
- c. Technology and Information Rulebook; and
- d. Market Conduct Rulebook.

3. For the avoidance of doubt, all Rules in Rulebooks apply cumulatively in addition to all other requirements in the Regulations, Rules and Directive and as such, in the event of overlap, the higher standard of compliance must be met at all times.

4. Licensing process. All Entities seeking a Licence from VARA to carry out Category 1 VA Issuance shall adhere to the licensing process as prescribed by VARA from time to time when applying for such Licence.

5. FRVA Rules. All Entities seeking to carry out the issuance of an FRVA will, in addition to compliance with all other Regulations, Rules and Directives as communicated by VARA in its Licence, or otherwise from time to time, be required to comply with the FRVA Rules in Annex 27 of this VA Issuance Rulebook at all times.

6. ARVA Rules. All Entity seeking to carry out the issuance of an ARVA will, in addition to compliance with all other Regulations, Rules and Directives as communicated by VARA in its Licence, or otherwise from time to time, be required to comply with the ARVA Rules in Annex 2 of this VA Issuance Rulebook, at all times.

7. Revocation or Suspension. VARA may, in its sole and absolute discretion, revoke a Licence for Category 1 VA Issuance in the event of any of the following—

- a. the Entity which has received the Licence has not issued the Virtual Asset within six (6) months after the approval has been granted;
- b. the Entity which has received the Licence obtained the Licence by making false or misleading statements including, but not limited to, in the Whitepaper, during the licensing process in Rule I.D.4 above, or in any other communications with VARA or the public;
- c. the Entity which has received the Licence no longer meets, or is in breach of, any of the conditions imposed by VARA in relation to the Licence;
- d. infringement of any Regulation, Rule or Directive;
- e. violation of any regulatory requirements applicable in other jurisdictions;
- f. the Entity which has received the Licence is Insolvent, subject to Insolvency Proceedings or otherwise has been put under an orderly wind-down plan in accordance with applicable insolvency laws;
- g. the Entity which has received the Licence has decided to stop its operations;
- h. on any ground on which VARA might refuse to issue a Licence;
- i. for Good Cause; or
- j. other grounds determined by VARA in exercising its powers, performing its functions or fulfilling its objectives under the Dubai VA Law.

8. Entities shall immediately notify VARA of any of the situations referred to in Rule I.D.7 of this VA Issuance Rulebook.

E. Category 2 VA Issuance

1. Entities in the Emirate may only issue Virtual Assets that fall within Category 2 above provided that, all placement and distribution is carried out by a Licensed Distributor.
2. Provided that Rule I.E.1 of this VA Issuance Rulebook is met, Entities in the Emirate that issue Virtual Assets that fall within Category 2 above do not need prior approval from VARA.

3. Licensed Distributors who provide Licensed Distribution Services to Issuers of Virtual Assets that fall within Category 2 above, assume the responsibility for assuring and validating that the Issuer complies with this VA Issuance Rulebook.
4. Licensed Distributors who provide Licensed Distribution Services to Issuers of Virtual Assets that fall within Category 2 above, must continue to comply with all other applicable Regulations, Rules and Directives, as well as any conditions of their Licence, at all times when providing such services.
5. No Virtual Asset issued under Category 2 shall be deemed in any way to have been approved by VARA and may not be construed or considered as such. VARA makes no representation and does not provide any warranties regarding any Issuer or Virtual Asset including, but not limited to, their fitness for purpose, suitability or regulatory status in any jurisdiction.

F. Exempt VAs

1. Entities in the Emirate may issue Exempt VAs without prior approval from VARA, provided that, they comply with Part II of this VA Issuance Rulebook at all times.
2. Issuers of Exempt VAs issued in accordance with Rule I.F.1 of this VA Issuance Rulebook shall remain subject to VARA's supervision, examination and enforcement at all times, in accordance with Part IV of this VA Issuance Rulebook.

Part II – General Rules

1. All Entities in the Emirate carrying out the issuance of any Virtual Asset shall comply with the following general Rules, at all times, when conducting all their business from or in the Emirate, including issuing any Virtual Asset—
 - a. *Integrity, honesty and fairness*: All Issuers should act fairly, clearly and in good faith, so as to not mislead and to serve the best interests of owners of the Virtual Assets they issue and preserve market integrity. Issuer shall use clear and transparent wording in all communications and public disclosures, treat all owners of the Virtual Asset fairly, and engage in ethical market practices;
 - b. *Diligence*: All Issuers must act with the due skill, care and diligence reasonably expected of an Issuer taking into the account the nature of the Virtual Asset;
 - c. *Capabilities and resource*: All Issuers must have and effectively employ the necessary resources (including technical, financial and otherwise), for the sound, effective and efficient operation of the issuance taking into the account the nature of the Virtual Asset, as well as all applicable legal and regulatory requirements;
 - d. *Effective communication and disclosures*: All Issuers must ensure that all communications and disclosures, including but not limited to those applicable in Part III of this VA Issuance Rulebook, are clear, concise, effective and contain all information necessary for owners and/or prospective owners of the Virtual Asset to make an informed decision and be kept up-to-date. All Issuers should dispatch information in a timely manner if ongoing disclosure is required by any relevant authorities including, but not limited to, VARA;
 - e. *Legal and regulatory compliance*: All Issuers must comply with all applicable laws and regulatory requirements in the UAE and as may apply to their business or operations in any jurisdiction at all times including, but not limited to, consumer protection laws; and
 - f. *Environmental responsibility*: All Issuers must act in an environmentally responsible manner including, but not limited to, mitigating negative environmental impacts of the Virtual Asset and disclosing how they identify, assess and manage other climate-related risks relevant to

the issuance and/or project lifecycle of the Virtual Asset.

Part III – Whitepapers and Public Disclosures

A. Application

1. All Entities in the Emirate issuing a Virtual Asset must comply with this Part III of the VA Issuance Rulebook, and publish both a Whitepaper and a Risk Disclosure Statement.
2. The only exception to Rule III.A.1 of this VA Issuance Rulebook is that Issuers of Exempt VAs do not need to publish a Whitepaper or a Risk Disclosure Statement in respect of Exempt VAs only.

B. Whitepapers

1. Initial Whitepaper. Prior to issuing a Virtual Asset, all Entities in the Emirate issuing a Virtual Asset shall provide the relevant disclosures set out in Schedule 1 of this VA Issuance Rulebook in a single easily accessible location in a machine-readable format, or in any form as may be prescribed by VARA from time to time (“**Whitepaper**”).
2. In addition to the relevant disclosures set out in Schedule 1 of this VA Issuance Rulebook, Issuers of any Category 1 VA Issuance will be required to include all additional information in the Whitepaper that is stipulated in any Annex applicable to the type of Virtual Asset being issued, as may be stipulated by VARA from time to time.
3. No Issuer may exclude, or attempt to exclude, any form of actual or potential civil liability in respect of any information in any Whitepaper, or any other disclosure or communication.
4. Issuers must publish the Whitepaper prior to making the Virtual Asset available to the public, including any offer or Marketing. The Whitepaper shall remain subject to all Rules set out in this VA Issuance Rulebook for as long as the Virtual Asset is available to the public.
5. Whitepaper updates. Issuers must ensure the Whitepaper is accurate and complete at all times including, but not limited to, making any necessary changes to the Whitepaper, or publishing an updated Whitepaper, in the event of changes to the Virtual Asset.
6. Issuers must take all reasonable steps to ensure owners of Virtual Assets are notified of any changes to a Virtual Asset prior to any such changes taking effect, except in the event an Issuer needs to implement any changes in response to a security or other threat, or which is in the best interests of maintaining the integrity of the Virtual Asset.
7. In the event of any update to the Whitepaper, Issuers must clearly state the date on which the Whitepaper has been updated and ensure all previous versions remain easily accessible in the same format and location in which they were initially published. Records of all versions of the Whitepaper must be kept for a minimum of eight (8) years, starting from the date on which the Virtual Asset ceases to be in circulation.

C. Risk Disclosure Statements

1. Initial Risk Disclosure Statement. Issuers must publish a statement that includes a detailed description of all material risks related to the Virtual Assets being issued as applicable in a machine-readable format (“**Risk Disclosure Statement**”). The Risk Disclosure Statement shall be drawn up as a document written in a concise manner, in a language that is clear, non-technical and comprehensible for owners of the Virtual Asset. Risk Disclosure Statements shall be made available in the same easily accessible location as, but remain separate from, the Whitepaper.

2. **Risk Disclosure Statement updates.** Issuers must ensure the Risk Disclosure Statement is accurate and complete at all times including, but not limited to, making any necessary updates to the Risk Disclosure Statement, or publishing an updated Risk Disclosure Statement, in the event of changes to the Virtual Asset.
3. In the event of any update to the Risk Disclosure Statement, Issuers must clearly state the date on which the Risk Disclosure Statement has been updated, and ensure all previous versions remain easily accessible in the same format and location in which they were initially published. Records of all versions of the Whitepaper must be kept for a minimum of eight (8) years, starting from the date on which the Virtual Asset ceases to be in circulation.

Part IV – Supervision, Examination and Enforcement

1. Issuers are reminded that under the Dubai VA Law and the Regulations, VARA has supervisory, examination and enforcement powers in relation to all Virtual Assets and VA Activities in the Emirate.
2. In respect of any Virtual Asset, including all categories specified in this VA Issuance Rulebook, which has already been issued or in the process of being issued, VARA may require an Issuer to suspend issuing the Virtual Asset, or issuing further Virtual Assets, if VARA believes a Virtual Asset, how it is being issued or the Issuer does not comply with any aspect of this VA Issuance Rulebook. VARA may also impose additional conditions and/or take further enforcement action within its power including, but not limited to, imposing fines or penalties.
3. Issuers must provide VARA with any books or other records requested by VARA to facilitate any examination of and/or investigation into the Issuer's compliance with its obligations under the Regulations including, but not limited to, this VA Issuance Rulebook.
4. Issuers shall ensure that VARA is granted all access as requested by VARA to perform its supervision, examination and enforcement responsibilities including, but not limited to—
 - a. immediate access to all premises, data, books and records throughout the period of VARA's examination;
 - b. all assistance necessary to ensure immediate access including authentication or approvals; and
 - c. ensure that doing so does not violate the local laws of any other jurisdiction in which the Issuer operates.

Schedule 1 – VA Whitepaper Requirements

A. Application

1. In accordance with **Part III** of this VA Issuance Rulebook, all Entities in the Emirate issuing a Virtual Asset must publish a Whitepaper, except in respect of Exempt VAs only.
2. The following table lists the information that Issuers and/or their Licensed Distributors must first consider as a minimum for each Virtual Asset when creating the Whitepaper.
3. VARA recognises that upon consideration of each item in the table by Issuers and/or their Licensed Distributors, not all of the information listed in this table will be applicable for every Virtual Asset. At such time, Issuers and/or their Licensed Distributors must exercise professional judgement, acting in accordance with the General Rules in **Part II** of this VA Issuance Rulebook at all times, when determining if the information listed in this table is applicable for the purposes of inclusion in a Whitepaper of a specific Virtual Asset.

4. If an Issuer and/or their Licensed Distributor fails to include any of the information listed in the table below in a Whitepaper, and it is later found that the information was applicable, then the Whitepaper does not comply with this VA Issuance Rulebook.
5. VARA will not be responsible for confirming, and will not accept requests to confirm, the applicability of any of the areas listed in the table to any Virtual Asset or Whitepaper. Issuers and/or their Licensed Distributors shall be fully responsible for the accuracy and completeness of all Whitepapers.

B. Whitepaper Requirements

A.	Information about the Issuer
i.	the Issuer's name, legal structure, registered address, and head office location (if different);
ii.	the Issuer's date of incorporation or registration;
iii.	the identity of the Issuer's parent company;
iv.	the identities, business addresses, and functions of the Issuer's owners, management and/or members;
v.	whether any individual involved in the issuance, including the Issuer's owners, management and/or members, has been convicted of any offence of dishonesty, fraud, financial crime or an offence under laws relating to companies, banking, insolvency, money laundering and insider dealing, and, to the extent permissible under applicable laws, whether any individual is subject to ongoing inquiries or investigations in respect of such offences;
vi.	the business, business related and/or professional activities of the Issuer, including any regulatory authorisations or Licences, and its group;
vii.	the Issuer's financial condition over the past three (3) years, or since registration if the Issuer has existed for less than three years;
viii.	an assessment based on a fair review of the development, performance, and position of the Issuer's business over the past three (3) years, or since registration if the Issuer has existed for less than three (3) years, including the causes of any material changes. The assessment should be a balanced and comprehensive analysis of the Issuer's business development, performance, and position, and should be consistent with the size and complexity of the business;
ix.	a detailed description of the Issuer's governance arrangements;
x.	if the Issuer issues other Virtual Assets or undertakes other Virtual Assets Activities, this should be clearly stated;
xi.	if there is any connection between the Issuer itself and the Entity or organisation that has control of the DLT used to issue the Virtual Assets, including if the DLT is run, managed or controlled by an Entity closely connected to the Issuer or other project participants; and
xii.	details of all Entities (including businesses addresses or company domiciles) involved in the issuance and/or operation of the Virtual Asset, such as advisors, development teams, and/or VASPs.
B.	Information about the Virtual Asset
i.	the name, abbreviation or ticker handler of the Virtual Asset;
ii.	a description of the characteristics of the Virtual Asset and all features and uses;
iii.	information about the plans for the Virtual Asset and all related projects, including a description of the past and future milestones and resources already allocated;

iv.	an explanation of the target market of the Virtual Asset, including any restrictions as regards the type of owners;
v.	the name of any trading platform for Virtual Assets where admission to trading is or will be sought, and information about how investors can access such trading platforms and the costs involved;
vi.	information about technical requirements necessary to own and/or hold the Virtual Asset, including but not limited the types of VA Wallets with which the Virtual Asset is compatible;
vii.	a detailed description of the issuance structure of the Virtual Asset, in particular the number that will be issued, the issuance schedule, when all of the supply of the Virtual Asset will be made available and how many will be allocated or retained by any party, including but not limited to the Issuer, its investors and/or advisors; and
viii.	the planned use of any proceeds or consideration received by the Issuer, in any form, related to issuing the Virtual Asset.
C.	Information about the rights and obligations attached to the Virtual Asset
i.	a description of the characteristics and functionality of the Virtual Asset being issued, including information about whether the functionality will change, and if so when such changes will take place;
ii.	a description of the rights and obligations, if any, of the owner, and the procedure and conditions for the exercise of those rights;
iii.	whether the rights represented by the Virtual Asset may differ depending on what DLT or platform the Virtual Asset is acquired or used;
iv.	a description of the conditions under which the rights and obligations may be modified;
v.	information on subsequent issuances or offers that may have a dilutive effect on the Virtual Asset being issued, and the number of units of the Virtual Asset retained by the Issuer itself;
vi.	information on how and where the Virtual Asset can be purchased or sold after the issuance;
vii.	any restrictions on the transferability, or additional steps required to give legal effect to a transfer of ownership, of the Virtual Asset that is being issued;
viii.	a description of protection schemes protecting the value of the Virtual Asset or any initial investments in the Virtual Asset;
ix.	information on the nature and enforceability of rights, including permanent rights of redemption and any claims that owners may have against the Issuer;
xii.	information on the arrangements put in place by the Issuer to ensure the liquidity of the Virtual Asset, including the name of the Entities in charge of ensuring such liquidity;
xiii.	the contact details for submitting complaints, and a description of the complaints-handling procedures and any dispute resolution mechanism or redress procedure established by the Issuer of the Virtual Asset;
xiv.	detailed information on any rights of redemption and how the Virtual Asset is redeemed, including whether the owner will be able to choose the form of redemption, the form of transference, or the official currency of redemption;
xv.	any material legal or regulatory considerations applicable to owning, storing, transferring, or otherwise using the Virtual Asset, including to give legal effect to a transfer of ownership; and
xvi.	the law applicable to the Virtual Asset, as well as the competent court.
D.	Information about underlying technology

i.	information on the technology used, including DLTs, as well as protocols and technical standards, allowing for the holding, storing, and transfer of Virtual Assets;
ii.	information on the consensus mechanism used by the DLT on which the Virtual Asset is issued including, where the Virtual Asset is issued on more than one DLT whether any variances in mechanisms used by different DLTs give rise to a variance in the rights of owners of the Virtual Asset;
iii.	incentive mechanisms to secure transactions and any applicable fees;
iv.	if the Virtual Asset is issued, transferred, and stored using DLT that is operated by the Issuer or a third-party acting on the Issuer's behalf, a detailed description of the functioning of such DLT and information on the outcome of any audits, if such an audit was conducted, including what Entity carried out the audit; and
v.	a statement on the environmental and climate-related impact of the Virtual Asset.
E.	Information about the Licensed Distributor
i.	name;
ii.	legal form;
iii.	registered address and head office, where different;
iv.	VARA Licence number;
v.	the name of the parent company; and
vi.	business or professional activity of the Licensed Distributor and of its parent company.
F.	Information about any initial offer to the public of the Virtual Asset
i.	the reasons for any offer to the public;
ii.	the amount that the offer to the public intends to raise denominated in AED, including any minimum and maximum target subscription goals set for the offer to the public of the Virtual Asset;
iii.	whether oversubscriptions are accepted and how allocations will be determined in the event of oversubscription;
iv.	a specific notice that purchasers participating in the offer to the public of Virtual Asset will be reimbursed if the minimum target subscription goal is not reached at the end of the offer to the public, or if the offer is cancelled, and a detailed description of the refund mechanism, including the expected timeline of when such refunds will be completed;
v	the issue price of the Virtual Asset being offered to the public, denominated in both AED and/or any other Virtual Assets;
vi.	the total number of Virtual Assets to be offered to the public, and the percentage of the total supply in circulation (i.e. supply available prior to the intended new issuance) of the Virtual Asset that the offer to the public represents;
vii.	an indication of the prospective owners targeted by the offer to the public, including any restriction as regards the type of owners for such Virtual Assets;
viii.	information about the various phases of the offer to the public of Virtual Assets, including information on discounted purchase prices for early purchasers of Virtual Assets (pre-public sales). In the case of discounted purchase prices for some purchasers, an explanation why purchase prices may be different, and a description of the impact on the other investors;
ix.	for time-limited offers, the subscription period during which the offer to the public is open;
x.	arrangements to safeguard funds or other Virtual Assets during the time-limited offer to the public or during the withdrawal period;
xi.	methods of payment to purchase the Virtual Assets offered, and methods of transfer of the value to the purchasers when they are entitled to be reimbursed;
xii.	information on any rights the Issuer has to withdraw or cancel the offer to the public;

xiii.	information on the manner and time schedule of transferring the purchased Virtual Assets to the owners and/or holder;
xiv.	expenses to be incurred by purchasers of the Virtual Asset related to the offer to the public of the Virtual Asset, including any applicable subscription fee or the method in accordance with which the offer price will be determined;
xv.	potential conflicts of interest of the persons involved in the offer to the public arising in relation to the offer; and
xvi.	the law applicable to the offer to the public of Virtual Assets, as well as the competent court.

Schedule 2 – Definitions

Term	Definition
“Anonymity-Enhanced Cryptocurrencies”	has the meaning ascribed to it in the Regulations.
“Asset Referenced Virtual Asset” or “ARVA”	means any Virtual Asset, that is not an FRVA, and which— (a) represents, or purports to represent, direct, indirect, current, future or contingent ownership of any RWA; (b) represents, or purports to represent, direct, indirect, current, future or contingent entitlement to receive or share any Income; (c) purports to maintain a stable value or reference to any type or combination of RWA(s) or Income; (d) represents, or purports to represent, entitlement to receive or share any value that is, or purports to be, or in any manner originate from, derived from or backed by (including but not limited to under any securitisation, collateralisation, or guarantee arrangement) any type or combination of RWA or Income; or (e) is a directly or indirectly wrapped, duplicated, fractionalised, securitised or derivative version of any other ARVA.
“ARVA Rules”	means the Asset-Referenced Virtual Assets Issuance Rules in <u>Annex 2</u> of this VA Issuance Rulebook.
“Broker-Dealer Services”	has the meaning ascribed to it in <u>Schedule 1</u> of the Regulations.
“Broker-Dealer Services Rulebook”	means the Broker-Dealer Services Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Category 1”	has the meaning ascribed to it in Rule <u>I.C.1</u> of this VA Issuance Rulebook.
“Category 1 VA Issuance”	means the VA Activity of issuing any Virtual Asset that falls within Category 1.
“Category 2”	has the meaning ascribed to it in Rule <u>I.C.1</u> of this VA Issuance Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Risk Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Directive”	has the meaning ascribed to it in the Regulations.

“Distributed Ledger Technology” or “DLT”	has the meaning ascribed to the term ‘Distributed Ledger Technology’ in the Dubai VA Law.
“Dubai VA Law”	means <u>Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</u> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Exempt VAs”	has the meaning ascribed to it in Rule <u>I.C.1</u> of this VA Issuance Rulebook.
“Fiat-Referenced Virtual Asset” or “FRVA”	means a Virtual Asset that purports to maintain a stable value in relation to the value of one or more fiat currencies, or one or more other FRVA(s), but does not have legal tender status in the UAE, and is not issued for use as a means of payment for goods or services in the UAE. An FRVA is neither issued nor guaranteed by any jurisdiction and fulfils its functions only by use and acceptance within the community of users of the FRVA. For the avoidance of doubt, and as stated in Rule <u>I.B.4</u> of the FRVA Rules, the issuance of any FRVA that purports to maintain a stable value in relation to the value of AED shall not be approved under this VA Issuance Rulebook or the FRVA Rules, and shall remain under the sole and exclusive regulatory purview of the CBUAE.
“FRVA Rules”	means the Fiat-Referenced Virtual Assets Issuance Rules in <u>Annex 1</u> of this VA Issuance Rulebook.
“Good Cause”	has the meaning ascribed to it in the Regulations.
“Income”	means sales proceeds, interests, dividends, profits, repayments or any other form of direct, indirect, current, future or contingent value originating or deriving from an RWA.
“Insolvency Proceedings”	has the meaning ascribed to it in the Regulations.
“Insolvent”	has the meaning ascribed to it in the Regulations.
“Issuer”	means the Entity responsible for the issuance of a Virtual Asset.
“Licence”	has the meaning ascribed to it in the Regulations.
“Licensed”	means having a valid Licence.
“Licensed Distribution Services”	has the meaning ascribed to it in the Broker-Dealer Services Rulebook.
“Licensed Distributor”	means a VASP Licensed by VARA to carry out Broker-Dealer Services.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Marketing”	has the meaning ascribed to it in the Marketing Regulations.
“Marketing Regulations”	means the <u>Regulations on the Marketing of Virtual Assets and Related Activities 2024</u> issued by VARA, as may be amended from time to time.
“Non-Transferable Virtual Asset”	means a Virtual Asset that— (a) is not sold by the Issuer for, and cannot be converted into, exchanged or redeemed for, fiat currency, Virtual Assets or any value in kind;

	<p>(b) is not redeemable or exchangeable for goods, services, discounts, purchases or otherwise has no market, use, or application; and</p> <p>(c) cannot be transferred between VA Wallets.</p>
“PDPL”	means the <i>Federal Decree-Law No. (45) of 2021 on the Protection of Personal Data</i> .
“Personal Data”	has the meaning ascribed to it in the PDPL.
“Redeemable Closed-Loop Virtual Asset”	<p>means a Virtual Asset that can be redeemed or exchanged for goods, services, discounts, or purchases with the Issuer and/or other merchants designated by the Issuer, provided that—</p> <p>(a) the Issuer is the legal owner and/or has validly enforceable legal right to grant all rights of redemption;</p> <p>(b) the Virtual Asset is not sold or exchanged for, and cannot be converted into, exchanged or redeemed for, fiat currency or Virtual Assets;</p> <p>(c) cannot be used or accepted as a means of payment outside of the closed-loop of the Issuer and/or other merchants designated by the Issuer; and</p> <p>(d) cannot be transferred between VA Wallets other than for the purposes of redemption from the Issuer or designated merchants.</p>
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended from time to time.
“Risk Disclosure Statement”	has the meaning ascribed to it in Rule <u>III.C.1</u> of this VA Issuance Rulebook.
“Rule”	has the meaning ascribed to it in the Regulations.
“RWA”	<p>means, in respect of any Virtual Asset, any type or combination of—</p> <p>(a) interest in any financial instrument, scheme or arrangement;</p> <p>(b) physical and/or tangible asset; or</p> <p>(c) intangible asset, rights or interest, other than—</p> <p>i. the Virtual Asset itself; or</p> <p>ii. items that exist in digital form only.</p>
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“UAE”	means the United Arab Emirates.
“VA Activity”	means the activities listed in <u>Schedule 1</u> of the Regulations, as may be amended from time to time.
“VA Issuance Rulebook”	means this Virtual Asset Issuance Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“VA Wallet”	has the meaning ascribed to the term ‘Virtual Asset Wallet’ in the Dubai VA Law.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.

“Whitepaper”	has the meaning ascribed to it in Rule <u>III.B.1</u> of this VA Issuance Rulebook.
“Working Day”	has the meaning ascribed to it in the Regulations.

Annex 1: Fiat-Referenced Virtual Assets Issuance Rules

Part I – Approval Requirements

A. Interpretation

1. “**Fiat-Referenced Virtual Asset**” or “**FRVA**” has the meaning ascribed to it in Schedule 2 – Definitions of the VA Issuance Rulebook.
2. As stated in Rule I.B.4 of these FRVA Rules, the issuance of any FRVA that purports to maintain a stable value in relation to the value of AED shall not be approved under these FRVA Rules and shall remain under the sole and exclusive regulatory purview of the CBUAE.
3. FRVAs do not include Virtual Assets which are—
 - a. representations of any equity claim;
 - b. issued by central banks acting in their monetary authority capacity (e.g. CBDCs); or
 - c. tokenised bank deposits used only for interbank settlement purposes.
4. “**Reference Currency**” means, in relation to a FRVA, a VARA-approved fiat currency—
 - a. the value of which an FRVA purports to maintain a stable reference to;
 - b. which is controlled by a central bank of any country(ies) or territory(ies) which are not subject to any sanctions in accordance with Federal AML-CFT Laws;
 - c. which has the status of legal tender; and
 - d. which is required to be accepted within a given jurisdiction.
4. “**Reserve Assets**” means, for the purposes of these FRVA Rules, the pool of assets maintained in accordance with Rule III.B of these FRVA Rules and as approved by VARA. Reserve Assets are not Client Money or Client VAs, as defined in the Compliance and Risk Management Rulebook.

B. General Requirements for VARA Approval

1. As stated in Rule I.C.1 of the VA Issuance Rulebook, the issuance of an FRVA is a Category 1 VA Issuance and as such is a VA Activity. In addition to compliance with these FRVA Rules, and all other Regulations, Rules and Directives as communicated by VARA in its Licence or otherwise from time to time, all Entities seeking to carry out the issuance of an FRVA will be required to comply with the following Rulebooks—
 - a. Company Rulebook;
 - b. Compliance and Risk Management Rulebook;
 - c. Technology and Information Rulebook;
 - d. Market Conduct Rulebook; and

- e. VA Issuance Rulebook.
2. Approval of each FVRA. All VASPs Licensed by VARA to carry out Category 1 VA Issuance must obtain approval from VARA prior to issuing each Fiat-Referenced Virtual Asset.
3. Approval conditions. VARA may, in its sole and absolute discretion, impose conditions on any approvals granted for the issuance of an FRVA by a VASP including, but not limited to—
 - a. segregation of the VASP's business or operations in relation to VA issuances and any other VA Activities (or other businesses and activities, if applicable) by implementing and strictly enforcing policies and procedures;
 - b. provision of further information to demonstrate the VASP's ability to comply with any Regulation, Rule or Directive; and/or
 - c. any additions or modifications to requirements set out in any Regulation, Rule and/or Directive.
4. AED as Reference Currency. In addition to Regulation III.A.4, the issuance of any Virtual Asset that purports to maintain a stable value in relation to the value of AED shall remain under the sole and exclusive regulatory purview of the CBUAE. Entities seeking to issue any such Virtual Asset in the Emirate must comply with any applicable CBUAE regulation.
5. Use of FRVAs in VA ecosystem only. FRVAs issued under these FRVA Rules may only be used for the purchase and/or sale of assets in the VA ecosystem and may not be used as a means of payment for goods or services within the UAE.
6. Currencies of sanctioned countries or territories. VASPs may not have as a Reference Currency any currency issued by any country(ies) or territory(ies) which are subject to sanctions under Federal AML-CFT Laws.

C. Significant FRVA Issuers

1. VARA may, in its sole and absolute discretion, designate any VASP Licensed to issue an FRVA as a Significant FRVA Issuer at the time of granting a Licence or anytime thereafter.
2. In designating a VASP as a Significant FRVA Issuer, VARA may consider all factors relevant to the VASP and/or the FRVA issued by the VASP, including but not limited to—
 - a. the number of holders of the FRVA;
 - b. the value of circulating and/or outstanding supply of the FRVA;
 - c. the value of the Reserve Assets maintained by the VASP;
 - d. the number and value of transactions in the FRVA;
 - e. whether the VASP and/or its affiliates carry out any other VA Activity(ies) and/or financial services in the Emirate, or provide services similar to VA Activities and/or financial services in other jurisdictions;
 - f. interconnectedness with licensed financial institutions and/or VASPs; and/or
 - g. the business, structural and operational complexity of the VASP in relation to the FRVA issued by it.
3. VARA may, in its sole and absolute discretion, impose any Rules on a Significant FRVA Issuer in addition to those contained in the Rulebooks, which may include, but not be limited to, additional Rules on—
 - a. company structure and corporate governance;

- b. Paid-Up Capital, Net Liquid Assets, Insurance and/or Reserve Assets;
- c. audits, regulatory reporting and regulatory notifications; and/or
- d. any other matter as VARA deems appropriate.

Part II – Additional Disclosures

A. Additional Whitepaper Disclosures

1. In addition to all other disclosures required in Rule III.A of the VA Issuance Rulebook, VASPs Licensed to issue FRVAs must include the following in the Whitepaper—
 - a. the type(s) and composition of Reference Currency(ies);
 - b. whether the type(s) and composition of Reference Currency(ies) may change and, if so, the circumstances in which any such changes may take place and the consequential effect of such changes;
 - c. a clear and detailed policy on the creation and redemption of FRVAs in circulation and the consequence of such creation or redemption on the increase and decrease of the Reserve Assets;
 - d. the type(s) and composition of Reserve Asset(s), and methodology for valuing such Reserve Assets;
 - e. criteria for how Reserve Asset(s) are or will be identified;
 - f. the custody arrangement of the Reserve Assets including, but not limited to, the custodian(s) involved and how the VASP Licensed to issue FRVAs ensures it has timely access to Reserve Assets to process redemption requests in compliance with Rule III.C of these FRVA Rules;
 - g. a detailed description of how Reserve Assets are maintained, with reference to the requirements in Rule III.B of these FRVA Rules;
 - h. a detailed description of how they will comply with Rules relating to the handling of redemption requests in Rule III.C of these FRVA Rules, and all relevant risks which may affect their compliance;
 - i. the procedures and timeline for holders of FRVAs to redeem such FRVAs at par;
 - j. prominently state whether having a valid Client Agreement with the VASP Issuer is a condition for redemption of the FRVA directly from the VASP Issuer;
 - k. detailed assessments of risks relevant to the management, custody, investment and/or liquidation of the Reserve Assets, including, but not limited to, credit risk, market risk and liquidity risk, and policies and procedures to manage such risks for the purpose of processing redemption requests; and
 - l. any other relevant information as may be determined by VARA.

B. Additional Ongoing Disclosures

1. VASPs Licensed to issue FRVAs shall at least every month and in a clear, accurate and transparent manner disclose on their website the following information regarding whether an FRVA is at least one hundred percent (100%) backed by Reserve Assets—
 - a. the number and value of FRVAs in circulation; and
 - b. the value and composition of the Reserve Assets,

as independently audited in accordance with Rule III.D.1 of these FRVA Rules.

2. Disclosures in accordance with Rule II.B.1 of these FRVA Rules shall be accompanied by a statement confirming whether the FRVA is, for the period covered and at the time of the disclosure, at least one hundred percent (100%) backed by Reserve Assets in accordance with independent audit requirements in Rule III.D.1 of these FRVA Rules.
3. VASPs Licensed to issue FRVAs shall as soon as possible and in a clear, accurate and transparent manner disclose on their website any event that has or is likely to have a significant effect, directly or indirectly, on the market value of the FRVAs.

Part III – Additional Compliance Obligations of FRVA Issuers

A. Maintenance of Stable Backing

1. VASPs Licensed to issue FRVAs shall ensure that—
 - a. any increase in the circulating supply of the FRVA is always matched by a corresponding increase in the Reserve Assets; and
 - b. any decrease in the circulating supply of the FRVA is always matched by a corresponding decrease in the Reserve Assets.
2. VASPs Licensed to issue FRVAs shall ensure that any increase or decrease in the Reserve Assets required under Rule III.A.1 of these FRVA Rules is responsibly managed to avoid any adverse market impact in relation to the Reserve Assets.
3. VASPs Licensed to issue FRVAs shall, regardless of whether any third party(ies) are involved in the creation or redemption of the FRVA, comply with Rule III.A.2 of these FRVA Rules at all times.

B. Reserve Assets

1. VASPs Licensed to issue FRVAs shall, at all times, hold and maintain sufficient Reserve Assets such that the FRVA is at least one hundred percent (100%) backed by Reserve Assets.
2. VASPs Licensed to issue FRVAs shall only hold Reserve Assets denominated in the Reference Currency(ies) in—
 - a. cash or cash equivalents (including, but not limited to, central bank reserve deposits, bank deposits and CBDCs); or
 - b. highly liquid financial instruments with minimal market risk, credit risk and concentration risk, which are capable of being liquidated rapidly with minimal adverse market impact, including the following—
 - a. debt securities with residual maturity of ninety (90) days or less, issued by—
 - i. governments or central banks of the Reference Currency; or
 - ii. government agencies (local or international);
 - b. repurchase agreements with a maturity of seven (7) days or less which are backed by (i) above; and

- c. short-term government money market funds.
- 3. VASPs Licensed to issue FRVAs shall, at all times, manage Reserve Assets effectively and prudently, at least by—
 - a. maintaining Reserve Assets only with financial services firms (as agreed with VARA during the licensing process)—
 - i. appropriately and validly licensed and authorised to hold the specific type of Reserve Assets;
 - ii. having regard to counterparty risk and/or exposure in the event of failure or each financial services firm becoming Insolvent; and
 - iii. segregated from their own funds;
 - b. ensuring newly added Reserve Assets are held in accordance with their custody arrangements;
 - c. putting in place policies and procedures to ensure Reserve Assets can be promptly accessed and converted into the Reference Currency(ies) at all times, for the purpose of processing and completing any redemption requests in accordance with Rule III.C of these FRVA Rules; and
 - d. conducting regular risk assessments to evaluate the appropriateness of the composition of Reserve Assets (including, but not limited to, whether there is sufficient diversification in the types of Reserve Assets held) in ensuring compliance with Rule III.B.1 of these FRVA Rules.
- 4. VASPs Licensed to issue FRVAs shall, to the furthest extent permitted by applicable laws, hold Reserve Assets of an FRVA in such a manner that—
 - a. such Reserve Assets are legally segregated and remote from their own assets (including, but not limited to, any assets held in relation to other FRVAs) and do not form a part of their estate;
 - b. they would not be prevented or hindered from processing any redemption requests in accordance with Rule III.C of these FRVA Rules, at all times (including, but not limited to, ensuring such Reserve Assets are not rehypothecated, or subject to any pledges, encumbrances, right of set-off or counterclaim);
 - c. will not otherwise be subject to any recourse by their creditors, the custodian of the Reserve Assets or any other third parties, in particular in the event that they become Insolvent; and
 - d. VARA has the ability to direct the control, liquidation and distribution of all such Reserve Assets for the purposes of fulfilling its regulatory obligations.
- 5. VASPs Licensed to issue FRVAs shall work with VARA to structure agreements with financial services firms to ensure VARA has priority access to Reserve Assets, to the furthest extent permitted by applicable laws, for the purposes of VARA fulfilling its regulatory obligations.
- 6. Conflicts of interest. In addition to all requirements relating to the avoidance and management of conflicts of interest in the Company Rulebook, VASPs Licensed to issue FRVAs shall take all appropriate steps, to the extent practicable, to prevent and, in any event identify, manage and publicly disclose conflicts of interest arising from the constitution and management of Reserve Assets.
- 7. It is worth noting that Reserve Assets held with financial services firms, including but not limited to those regulated by the CBUAE, may be subject to prevailing reporting obligations incremental

to those applicable under this Rulebook.

C. Redemptions

1. VASPs Licensed to issue FRVAs shall, at all times, ensure holders of the FRVA have the valid legally enforceable right to redeem the FRVA at par.
2. VASPs Licensed to issue FRVAs must ensure all requests made by holders, with valid Client Agreements with the VASP Issuer, to redeem the FRVA at par are, at all times, processed and completed—
 - a. within one (1) Working Day of any such requests; or
 - b. if the trading and/or settlement of the Reserve Assets are subject to significant disruption events beyond the control of a VASP Licensed to issue FRVAs, within one (1) Working Day of the trading and/or settlement of Reserve Assets no longer being significantly impacted by such disruption events.
3. VASPs Licensed to issue FRVAs shall process and complete redemption requests without charging any fees.
4. VASPs Licensed to issue FRVAs shall establish, maintain and implement clear and detailed policies and procedures to ensure compliance with this Rule III.C of these FRVA Rules.

D. Audits and Reporting

1. In addition to all requirements relating to audits and reporting in the Compliance and Risk Management Rulebook, VASPs Licensed to issue FRVAs shall, on a monthly basis, commission an independent audit of the following information regarding whether an FRVA is one hundred percent (100%) backed by Reserve Assets—
 - a. the number and value of FRVAs in circulation; and
 - b. the composition and value of Reserve Assets.
2. The Senior Management of a VASP Licensed to issue FRVAs shall, as soon as practicable upon its completion, submit to VARA an attestation as to the accuracy of each independent audit in accordance with Rule III.D.1 of these FRVA Rules.

E. Marketing

1. No Entity may, in the Marketing of any FRVA in the Emirate, include language suggesting that the value of an FRVA is maintained stable relative to its Reference Currency(ies), unless—
 - a. it has a Licence to issue the FRVA and such Licence has not been revoked; and
 - b. the FRVA was issued and is maintained in accordance with these FRVA Rules.
2. VASPs Licensed to issue FRVAs shall, in all Marketing, include clear and unambiguous statements that—
 - a. the holders of the FRVA have the right to redeem the FRVA at par, and whether such right is directly enforceable against the VASP Issuer; and

b. such FRVAs are not covered by any investor protection or deposit guarantee schemes.

F. Capital Requirements

1. VASPs Licensed to issue FRVAs shall always maintain Paid-Up Capital equal to the total of—
 - a. AED 1,500,000; and
 - b. two percent (2%) of the value of available supply of the FRVA.

Schedule 1 – Definitions

Term	Definition
“Category 1 VA Issuance”	has the meaning ascribed to it in the VA Issuance Rulebook.
“CBDC”	has the meaning ascribed to it in the Regulations.
“CBUAE”	means the Central Bank of the United Arab Emirates.
“Client Agreements”	has the meaning ascribed to it in the Market Conduct Rulebook.
“Client Money”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Client VA”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Company Rulebook”	means the Company Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Compliance and Management Rulebook”	means the Compliance and Risk Management Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Directive”	has the meaning ascribed to it in the Regulations.
“Dubai VA Law”	means <i>Dubai Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</i> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Federal AML-CFT Laws”	has the meaning ascribed to it in the Regulations.
“Fiat-Referenced Virtual Asset” or “FRVA”	has the meaning ascribed to it in <u>Schedule 2 – Definitions</u> of the VA Issuance Rulebook.
“FRVA Rules”	means these Fiat-Referenced Virtual Assets Issuance Rules issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Group”	has the meaning ascribed to it in the Company Rulebook.
“Insolvency Proceedings”	has the meaning ascribed to it in the Regulations.
“Insolvent”	has the meaning ascribed to it in the Regulations.
“Insurance”	has the meaning ascribed to it in the Company Rulebook.
“Market Conduct Rulebook”	means the Market Conduct Rulebook issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Marketing”	has the meaning ascribed to it in the Marketing Regulations.

“Marketing Regulations”	has the meaning ascribed to it in the VA Issuance Rulebook.
“Net Liquid Assets”	has the meaning ascribed to it in the Company Rulebook.
“Paid-Up Capital”	has the meaning ascribed to it in the Company Rulebook.
“Reference Currency”	has the meaning ascribed to it in Rule <u>I.A.4</u> of these FRVA Rules.
“Regulations”	means the <u>Virtual Assets and Related Activities Regulations 2023</u> , as may be amended or supplemented by VARA from time to time.
“Reserve Assets”	has the meaning ascribed to it in Rule <u>I.A.5</u> of these FRVA Rules.
“Senior Management”	has the meaning ascribed to it in the Company Rulebook.
“Significant FRVA Issuer”	means a VASP designated by VARA in accordance with Rule <u>I.C.1</u> of these FRVA Rules.
“Technology and Information Rulebook”	means the Technology and Information Rulebook issued by VARA pursuant to the Regulations, as may be amended VARA from time to time.
“VA Issuance Rulebook”	means the Virtual Asset Issuance Rulebook issued by VARA pursuant to the Regulations, as may be amended or supplemented by VARA from time to time.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.
“Whitepaper”	has the meaning ascribed to it in the VA Issuance Rulebook.
“Working Day”	has the meaning ascribed to it in the Regulations.

Annex 2: Asset-Referenced Virtual Assets Issuance Rules

Part I – Approval Requirements

A. Interpretation

1. **“Asset-Referenced Virtual Assets” or “ARVAs”** has the meaning ascribed to it in Schedule 2 – Definitions of the VA Issuance Rulebook.
2. **“Income”** has the meaning ascribed to it in Schedule 2 – Definitions of the VA Issuance Rulebook.
3. **“Reference Assets”** means, in relation to an ARVA, the RWA and/or Income the ARVA represents or purports to represent, as approved by VARA.
4. **“Reserve Assets”** means, for the purposes of these ARVA Rules, the asset or assets maintained in accordance with Rule III.C of these ARVA Rules and as approved by VARA. Reserve Assets are not Client Money or Client VAs, as defined in the Compliance and Risk Management Rulebook.
5. **“RWA”** has the meaning ascribed to it in Schedule 2 – Definitions of the VA Issuance Rulebook.

B. General Requirements for VARA Approval

1. As stated in Rule I.C.1 of the VA Issuance Rulebook, the issuance of an ARVA is a Category 1 VA Issuance and as such is a VA Activity. In addition to compliance with these ARVA Rules, and all other Regulations, Rules and Directives as communicated by VARA in its Licence or otherwise

from time to time, all Entities in the Emirate seeking to issue an ARVA will be required to comply with the following Rulebooks—

- a. Company Rulebook;
- b. Compliance and Risk Management Rulebook;
- c. Technology and Information Rulebook;
- d. Market Conduct Rulebook; and
- e. VA Issuance Rulebook.

2. Approval of each ARVA. All VASPs Licensed by VARA to carry out Category 1 VA Issuance must obtain approval from VARA prior to issuing each ARVA.
3. Approval conditions. VARA may, in its sole and absolute discretion, impose conditions on any approvals granted for the issuance of an ARVA by a VASP, including, but not limited to—
 - a. segregation of the VASP's business or operations in relation to VA issuances and any other VA Activities (or other businesses and activities, if applicable) by implementing and strictly enforcing policies and procedures;
 - b. obtaining and maintaining all necessary regulatory approvals and licences for activities involving the RWA and/or Reserve Assets, which must be carried out for the normal functioning of the ARVA, or otherwise provide further information to demonstrate ongoing compliance with all applicable laws and regulations;
 - c. provision of further information to demonstrate the VASP's ability to comply with any Regulation, Rule or Directive; and/or
 - d. any additions or modifications to requirements set out in any Regulation, Rule and/or Directive.
4. Applicable Rules. On receiving approval to issue an ARVA by VARA, a VASP will be required to comply with all Rules or requirements that VARA may impose on the VASP as a condition and ongoing requirement for any approval. VARA may impose Rules in addition to, or disapply any of, the Rules in these ARVA Rules depending on the considerations which it deems relevant to the nature of the ARVA being issued and/or the VASP. Any additional Rules imposed on a VASP may be requirements equivalent or similar to those contained in the Regulations, Rulebooks or Directives.

C. Significant ARVA Issuers

1. VARA may, in its sole and absolute discretion, designate any VASP Licensed to issue an ARVA as a Significant ARVA Issuer at the time of granting a Licence or anytime thereafter.
2. In designating a VASP as a Significant ARVA Issuer, VARA may consider all factors relevant to the VASP and/or the ARVA issued by the VASP, including but not limited to—
 - a. the number of owners and/or holders of the ARVA;
 - b. the value of circulating and/or outstanding supply of the ARVA;
 - c. the value of the Reserve Assets maintained by the VASP;
 - d. the number and value of transactions in the ARVA;
 - e. whether the VASP and/or its affiliates carry out any other VA Activity(ies) and/or financial services in the Emirate, or provide services similar to VA Activities and/or financial services in other jurisdictions;
 - f. interconnectedness with licensed financial institutions and/or VASPs; and/or

- g. the business, structural and operational complexity of the VASP in relation to the ARVA issued by it.

3. VARA may, in its sole and absolute discretion, impose any Rules on a Significant ARVA Issuer in addition to those contained in the Rulebooks, which may include, but not be limited to, additional Rules on—

- a. company structure and corporate governance;
- b. Paid-Up Capital, Net Liquid Assets, Insurance and/or Reserve Assets;
- c. audits, regulatory reporting and regulatory notifications; and/or
- d. any other matter as VARA deems appropriate.

Part II – Additional Disclosures

A. Additional Whitepaper Disclosures

1. In addition to all other disclosures required in the Part III of the VA Issuance Rulebook, VASPs Licensed to issue ARVAs must include the following in the Whitepaper—

- a. a clear and accurate description of the rights and/or value that the ARVA grants, or purports to grant, owners and/or holders of the ARVA and a clear and detailed policy on how the VASP ensures the ARVA derives and maintains its value;
- b. the types and composition of Reference Assets, and criteria for how such Reference Assets were identified;
- c. whether the types of Reference Asset will change and, if so, the circumstances in which any such changes may take place;
- d. whether the ARVA represents, or purports to represent, a direct right of ownership of the Reference Assets, or a fractional proportion thereof, and if so, a detailed description of how the right of ownership is established and/or such fractionalisation is structured;
- e. if transactions in the Reference Assets are subject to legal or regulatory requirements relating to their settlement and/or transfer of title, a detailed description of how such requirements will be met and an explanation of how the VASP will respond to transactions in the ARVA not resulting in corresponding transactions in the Reference Asset being legally settled, completed and/or transferred, and any mitigation employed by the VASP to address such risks;
- f. whether the ARVA maintains, or purports to maintain, a stable reference to the value of the Reference Assets, and if so, a detailed description of how such stable reference is maintained and the weighting of each type of Reference Asset in the unit value of the ARVA;
- g. whether the VASP will maintain Reserve Assets in respect of the ARVA;
- h. the types and composition of Reserve Assets (if applicable), and criteria for how such Reserve Assets were identified;
- i. whether the types of Reserve Asset may be subject to change and, if so, the circumstances in which any such changes may take place, including a detailed description of the VASP's investment policy for the Reserve Assets (if applicable);
- j. a clear and detailed policy on the procedure for the creation and destruction of the ARVAs in public circulation and the consequence of such creation or destruction on the increase and decrease of the Reserve Assets (if applicable);

- k. full details of the rights of owners and/or holders of the ARVA to redeem the value of the ARVA, including but not limited to the requirements under Rule III.E and the procedures and timeline for owners and/or holders of the ARVA to redeem such value;
- l. the custody arrangement of the Reference Asset and/or Reserve Assets, including but not limited to, the custodians involved and how the VASP ensures it has timely access to Reserve Assets to process redemption requests;
- m. detailed assessments of risks relevant to the management, custody, investment and/or liquidation of the Reference Asset and/or Reserve Assets, including but not limited to, credit risk, market risk, counterparty risk and liquidity risk, and policies and procedures to manage such risks for the purpose of processing redemption requests; and
- n. any other relevant information as may be determined by VARA.

B. Additional Ongoing Disclosures

- 1. VASPs Licensed to issue ARVAs shall at least monthly, and in a clear, accurate and transparent manner disclose on their website—
 - a. the number and value of ARVAs in public circulation; and
 - b. the value and composition of the Reserve Assets (if applicable).
- 2. Disclosures in accordance with Rule III.B shall be accompanied by a statement confirming whether or not the ARVA is, at the time of the disclosure, fully backed by sufficient Reserve Assets in accordance with Rule III.C.1.

Part III – Additional Compliance Obligations of ARVA Issuers

A. Value of an Asset-Referenced Virtual Asset

- 1. All Entities seeking to issue an ARVA shall clearly demonstrate to VARA—
 - a. the rights and/or value that the ARVA grants, or purports to grant, to the owners and/or holders of the ARVA; and
 - b. a clear and detailed policy on how the Entity will ensure the ARVA derives and maintains its value.
- 2. Reference Asset. All Entities seeking to issue an ARVA shall clearly demonstrate to VARA the type and composition of Reference Assets and whether the Reference Asset may change and, if so, the circumstances in which any such changes may take place.

B. Direct Right of Ownership

- 1. All VASPs Licensed to issue an ARVA which represents, or purports to represent, a direct right of ownership of the Reference Asset, or a fractional proportion thereof, shall ensure—
 - a. the right of ownership is legally and validly established and that such right of ownership is transferred in the event of a transfer of ownership of the ARVA;

- b. where transactions in the Reference Assets are subject to legal or regulatory requirements relating to their settlement, completion and/or transfer of title, that such legal or regulatory requirements are satisfied, in order to give effect to the transfer of ownership in the event of a transfer of ownership of the ARVA; and
- c. that the VASP will respond to transactions in the ARVA not resulting in a corresponding transaction in the Reference Asset being legally settled, completed and/or transferred, and shall implement mitigating measures to ensure all transactions in the ARVA result in a corresponding transaction in the Reference Asset being legally settled, completed and/or transferred.

2. Legal opinion. VASPs Licensed to issue ARVAs may be required to provide VARA with a legal opinion, provided by a professional and duly registered lawyer, confirming any explanation made either to VARA or any information contained in a Whitepaper.

C. Reserve Assets

- 1. VASPs Licensed to issue ARVAs which purport to maintain a stable value in respect of any Referenced Asset, shall hold and maintain sufficient and acceptable Reserve Assets such that—
 - a. the risks associated with the rights and/or to the value that the ARVA grants, or purports to grant, owners of the ARVA are secured; and
 - b. the liquidity risks associated with any rights of redemption granted to the owners and/or holders are mitigated and managed.
- 2. VASPs Licensed to issue ARVAs shall, at all times, manage Reserve Assets effectively and prudently, at least by—
 - a. maintaining Reserve Assets only with custodians or other Entities which are validly licensed and qualified to hold such assets;
 - b. ensuring Reserve Assets are segregated from the VASP's own funds;
 - c. ensuring newly added Reserve Assets are held in custody in accordance with Rule III.C.2.a by no later than the time period stipulated by VARA as a condition of its approval of the VASP to issue the ARVA;
 - d. having in place policies and procedures to ensure Reserve Assets can be promptly accessed to process and complete any redemption requests in accordance with Rule III.E, including but not limited to conversion into AED where the redemptions are being paid in AED; and
 - e. conducting regular risk assessments to evaluate the appropriateness of the composition of Reserve Assets in ensuring compliance with this Rule III.C .
- 3. VASPs Licensed to issue ARVAs shall, to the furthest extent permitted by applicable laws, ensure that Reserve Assets—
 - a. are legally segregated from its estate and the Reserve Assets of any other Virtual Assets;
 - b. are not rehypothecated, or subject to any pledges or encumbrances which would prevent the Issuer from processing any redemption request in accordance with Rule III.E; and
 - c. will not otherwise be subject to any recourse by the creditors of the VASP, the custodian of the Reserve Assets or any other third parties, in particular, in the event of any party

becoming Insolvent.

4. Legal opinion. VASPs Licensed to issue ARVAs shall be required to provide VARA with a legal opinion, provided by a duly registered practising lawyer, confirming compliance with Rule III.C.3 above.
5. Conflicts of interest. VASPs Licensed to issue ARVAs shall take all appropriate steps to prevent, identify, manage and publicly disclose conflicts of interest arising from the constitution and management of Reserve Assets.

D. Audits and Reporting

1. For the purposes of complying with this Rule III.D, VASPs Licensed to issue ARVAs shall appoint an independent third-party auditor and promptly notify VARA of the full name and contact details of the auditor upon appointment.
2. VASPs Licensed to issue ARVAs shall—
 - a. every six (6) months, commission an independent audit of—
 - a. the number and value of the ARVAs in public circulation;
 - b. the composition and value of the Reserve Assets, if applicable; and
 - b. commission an independent audit of their financial statements to produce an annual report, which shall be promptly made available to VARA upon request.
3. The Senior Management of the VASP Licensed to issue ARVAs shall, as soon as practicable upon its completion, submit to VARA an attestation as to the accuracy of each independent audit in accordance with Rule III.D of these ARVA Rules.

E. Redemptions

1. To the extent an ARVA provides owners and/or holders with a right of redemption, the VASP Licensed to issue the ARVA shall, at all times, ensure owners and/or holders of the ARVA have the right to redeem the ARVA for an equal value denominated in—
 - a. AED; and
 - b. other forms as may be determined by the VASP and disclosed in the Whitepaper.
2. To the extent an ARVA provides owners and/or holders with a right of redemption, the VASP Licensed to issue the ARVA shall, at all times, ensure owners and/or holders of the ARVA have the right to redeem the ARVA—
 - a. against the VASP; or
 - b. otherwise in respect of the Reserve Assets in the event that the VASP is unable to process and complete redemption requests.
3. VASPs Licensed to issue ARVAs must ensure all requests made by owners and/or holders to redeem such ARVAs for an equal value of RWAs shall be processed and completed within a reasonable period of such requests being made, provided the owner and/or holder, or their

designee, has successfully onboarded with the VASP and any other conditions necessary to permit redemption in compliance with all applicable laws, Regulations, Rules and Directives have been met.

4. VASPs Licensed to issue ARVAs shall process and complete redemption requests without charging any fees.
5. VASPs Licensed to issue ARVAs shall establish, maintain and implement clear and detailed policies and procedures to ensure compliance with this Rule III.E.

F. Marketing

1. No Entity may, in the Marketing of any Virtual Asset in the Emirate, use the term 'stablecoin' or include language suggesting that the value of a Virtual Asset is maintained stable relative to a particular RWA, unless—
 - a. it is a VASP Licensed by VARA to issue ARVAs and has received VARA's approval to issue the ARVA and such approval has not been revoked;
 - b. such ARVA purports to maintain a stable reference to the value of one RWA only; and
 - c. the VASP maintains Reserve Assets in accordance with Rule III.C of these ARVA Rules.
2. VASPs Licensed to issue ARVAs shall, in all Marketing relating to any ARVA, include clear and unambiguous statements that such ARVA is not covered by any investor protection or deposit guarantee schemes.

G. Capital Requirements

1. VASPs Licensed to issue ARVAs shall always maintain Paid-Up Capital equal to the value of at least the higher of—
 - a. AED 1,500,000; and
 - b. 2% of the average market value of the Reserve Assets (where applicable) calculated over the preceding twenty-four (24) months.

Schedule 2 – Definitions

Term	Definition
“Asset-Referenced Virtual Asset” or “ARVA”	has the meaning ascribed to it in <u>Schedule 2 – Definitions of the VA Issuance Rulebook</u> .
“ARVA Rules”	means these Asset-Referenced Virtual Assets Issuance Rules issued by VARA pursuant to the Regulations, as may be amended from time to time.
“Category 1 VA Issuance”	has the meaning ascribed to it in the VA Issuance Rulebook.
“Client Money”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Client VA”	has the meaning ascribed to it in the Compliance and Risk Management Rulebook.
“Directive”	has the meaning ascribed to it in the Regulations.

“Dubai VA Law”	means <i>Dubai Law No. (4) of 2022 Regulating Virtual Assets in the Emirate of Dubai</i> , as may be amended from time to time.
“Emirate”	means all zones across the Emirate of Dubai, including Special Development Zones and Free Zones but excluding the Dubai International Financial Centre.
“Entity”	means any legal entity or individual.
“Insolvency Proceedings”	has the meaning ascribed to it in the Regulations.
“Insolvent”	has the meaning ascribed to it in the Regulations.
“Issuer”	means the Entity responsible for the issuance of a Virtual Asset.
“Marketing”	has the meaning ascribed to it in the Marketing Regulations.
“Marketing Regulations”	means the <i>Regulations on the Marketing of Virtual Assets and Related Activities 2024</i> , issued by VARA and as may be amended or superseded from time to time.
“Regulations”	means the <i>Virtual Assets and Related Activities Regulations 2023</i> , as may be amended from time to time.
“Reference Assets”	has the meaning ascribed to it in Rule III.A.3 of these ARVA Rules.
“Reserve Assets”	has the meaning ascribed to it in Rule III.A.4. of these ARVA Rules.
“Senior Management”	means the executive management of an Entity responsible and accountable to the Board for the sound and prudent day-to-day management of the Entity, generally including but not limited to, the chief executive officer, chief financial officer, chief risk officer, and heads of the compliance and internal audit functions, or as equivalent roles may be titled.
“Significant ARVA Issuer”	means a VASP designated by VARA in accordance with Rule III.C.1 of these ARVA Rules.
“VA Issuance Rulebook”	means the Virtual Asset Issuance Rulebook issued by VARA pursuant to the Regulations, as may be amended or supplemented by VARA from time to time.
“VARA”	means the Dubai Virtual Assets Regulatory Authority.
“Virtual Asset” or “VA”	has the meaning ascribed to it in the Dubai VA Law.
“Whitepaper”	has the meaning ascribed to it in Rule III.A.1 of the VA Issuance Rulebook.