RULE AND STATEMENT OF GUIDANCE

Market Conduct for Virtual Asset Service Providers

February 2026

Table of Contents

List of Acronyms

CIMA	Cayman Islands Monetary Authority
MAA	Monetary Authority Act
MNPI	Material Non-Public Information
RSOG	Rule and Statement of Guidance
VA	Virtual Asset
VASPA	Virtual Asset Service Providers Act
VASPs	Virtual Asset Service Providers
VATP	Virtual Asset Trading Platform

Rule and Statement of Guidance

Market Conduct for Virtual Asset Services Providers

1. Introduction

1.1 This document ("The Rule and Statement of Guidance") establishes the Cayman Islands Monetary Authority's (the "Authority" or "CIMA") *Rule and Statement of Guidance on Market Conduct for Virtual Asset Service Providers* ("VASPs").

1.2 The Rule and Statement of Guidance ("RSOG") should be read in conjunction with:

(a) Monetary Authority Act ("MAA");

(b) Virtual Asset (Service Providers) Act (the "VASPA");

(c) Anti-Money Laundering Regulations;

(d) Guidance Notes on the Prevention and Detection of Money Laundering and Terrorist Financing in the Cayman Islands;

(e) Statement of Principles on Conduct of Virtual Asset Services;

(f) Rule on Obligations for the Provision of Virtual Asset Services Virtual Asset Custodians and Virtual Asset Trading Platforms;

(g) Statement of Guidance on Obligations for the Provision of Virtual Asset Services - Virtual Asset Custodians and Virtual Asset Trading Platforms;

(h) Statement of Guidance on Outsourcing for Regulated Entities;

(i) Regulatory Policy on Marketing Policies of Licensees;

(j) Rule and Statement of Guidance on Internal Controls for Regulated Entities;

(k) Rule on Corporate Governance for Regulated Entities;

(l) Rule on Cybersecurity for Regulated Entities;

(m) Statement on Cybersecurity for Regulated Entities;

(n) Statement of Guidance Nature, Accessibility and Retention of Records;

(o) The Regulatory Policy on Fitness and Propriety; and

(p) any other relevant Acts and regulatory instruments issued by the Authority from time to time.

1.3 To highlight the Authority's market conduct rules within the compendium, a rule is written in light blue and designated with the letter "R" in the right margin.

2. Statement of Objectives

2.1 This RSOG establishes minimum requirements and guidance for VASPs in relation to market conduct.

3. Statutory Authority

3.1 This RSOG is consistent with the Authority's statutory objectives as prescribed in Section 6(1)(b) of the MAA, which provides that the principal regulatory functions of the Authority are to:

"(i) to regulate and supervise financial services business carried on in or from within the Islands in accordance with this Law and the regulatory laws;
(ii) to monitor compliance with the anti-money laundering regulations; and
(iii) to perform any other regulatory or supervisory duties that may be imposed on the Authority by any other law;"

3.2 Additionally, section 34(1) of the MAA provides that:

"After private sector consultation and consultation with the Minister charged with responsibility for Financial Services, the Authority may–

(a) issue or amend rules or statements of principle or guidance concerning the conduct of Regulated Entity's and their officers and employees, and any other persons to whom and to the extent that the regulatory acts may apply;

(b) issue or amend statements of guidance concerning the requirements of the anti-money laundering regulations or the provisions of the regulatory laws; and

(c) issue or amend rules or statements of principle or guidance to reduce the risk of financial services business being used for money laundering or other criminal purposes."

4. Scope of Application

4.1 This RSOG applies to Regulated Entities that have been authorised by the Authority to conduct virtual asset services pursuant to the VASPA.

4.2 The Authority will assess Regulated Entities' compliance with this RSOG in a manner commensurate with the size, complexity, structure, nature of business and risk profile of its operations.

4.3 The Authority acknowledges that Regulated Entities that are part of a group may be subject to group-wide market conduct practices and that such Regulated Entities may rely on the group's policies in respect of certain market conduct matters. Where a Regulated Entity is part of a group, it may rely on the group market conduct framework provided that the Regulated Entity's Governing Body is satisfied that the framework is commensurate with the size, complexity, structure, nature of business and risk profile of the Regulated Entity's operations and that the framework meets the legal requirements in the Cayman Islands, including those outlined in this RSOG. Where gaps are identified, a tailored market conduct framework that complies with this RSOG and legal requirements in the Cayman Islands should be implemented.

4.4 References to any Act or Regulation should be construed as references to those provisions as commenced, amended, modified, re-enacted or replaced from time to time. For avoidance of doubt, this document applies to the acts or regulations to the extent that such provisions in those acts or regulations are in force.

5. Definitions

5.1 The following definitions are provided for the purpose of this Rule and Statement of Guidance:

5.1.1. The **"Authority"** has the same meaning as defined in the VASPA.

5.1.2. **"Agent"** refers to a person or entity that is authorised to act on behalf of a principal, whether for initiating transactions, handling documentation, or providing services, subject to the terms agreed with the principal and applicable law.

5.1.3. **"Client"** means a legal or natural person to whom virtual asset services are provided.

5.1.4. **"Client Agreement"** refers to a written document agreed to by the Client and the Regulated Entity, containing the conditions, terms of the business, and services provided to the Client by the Regulated Entity.

5.1.5. **"Communication Channels"** includes, but is not limited to, the Regulated Entity's official website, social media platforms, print or television media, email broadcasts, newsletters, and any other medium used to convey information to Clients and the public.

5.1.6. **"Control Functions"** mean properly authorised functions, whether in the form of a person, unit or department, serving a control or checks and balances function from a governance standpoint and which carry out specific activities, including strategy setting, risk management, compliance, actuarial matters, internal audit, and similar functions.

5.1.7. **"Cross-border transaction"** means any transaction where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of transactions that has at least one cross-border element.

5.1.8. **"Governing Body"** of a Regulated Entity is the Board of Directors where the entity is a corporation, the General Partner where the entity is a partnership, the manager where the entity is a Limited Liability Company, and the Board of Trustees where the entity is a trust business, or any equivalent governing structure as appropriate, taking into account the nature, size, and legal form of the Regulated Entity.

5.1.9. **"Issuance of Virtual Assets" or "Virtual Asset Issuance"** has the same meaning as defined in the VASPA.

5.1.10. **"Public Disclosures"** means information that a Regulated Entity makes available to the public regarding its operations, virtual asset services, processes and controls, and compliance standing with the legal, financial, and regulatory requirements in the Cayman Islands or in any other jurisdiction in which it conducts business.

5.1.11. **"Regulated Entity"** means any legal person or arrangement that has been granted a license, registration, or waiver in accordance with the VASP waiver.

5.1.12. **"Senior Management"** includes the most senior staff of the regulated entity, including heads of divisions, and any person who fulfils the functions of a senior manager, by whatever name called. Such functions include actively participating in the daily planning, supervision, administration and execution of a regulated entity's objectives and strategy.

5.1.13. **"Virtual Asset Custodian"** has the same meaning as defined in the VASPA.

5.1.14. **"Virtual Asset Trading Platform" ("VATP**") has the same meaning as defined in the VASPA.

A. General Guidelines and Requirements

6. Integrity and Conflicts of Interest

6.1 Regulated Entities are expected to act with honesty and integrity. The relationship between a Regulated Entity and its Clients should be based on the utmost good faith, by always upholding and acting within the terms of the documentation[1] governing their relationship and in accordance with applicable Acts and regulations.

6.2 A Regulated Entity must establish, document, and implement clear written policies and procedures to ensure that it acts in the best interest of its Clients, and fulfil the responsibilities that it has undertaken on behalf of its Clients. R

6.3 A Regulated Entity must conduct its business with due skill, care, and diligence, and must act ethically and professionally in a manner that safeguards the integrity of the market and prioritises the best interests of its Clients. Clients and prospective Clients must be treated fairly, transparently, and equitably. R

6.4 A Regulated Entity must conduct its business in accordance with the terms and any conditions of its licence or registration under the VASPA. R

6.5 The Authority will consider whether the Regulated Entity is acting within its powers and the specific virtual asset services for which a Regulated Entity has

[1] 'terms of documentation' is used in a broad context to refer to the Client Agreement as well as any contractual and operational documents that may govern the Client relationship. These may include, but are not limited to, onboarding disclosures, promotional, offering documentation, custodial terms, supplemental product terms, and risk acknowledgements.

been licensed or registered as the scope of activities authorised under its licence or registration; since, consistent with Section 4 of the VASPA, Regulated Entities are prohibited from carrying out any specific virtual asset service activity(ies) outside the scope of their approved licence or registration, regardless of whether such services are provided directly or through affiliated entities on behalf of the Regulated Entity.

6.6 A Regulated Entity must maintain the confidentiality of a Client's affairs and protect the privacy of the information obtained from Clients, unless disclosure is required or permitted under applicable Acts and regulations, or with the consent of such Client to whom the duty of confidentiality is owed. R

6.7 A Regulated entity should therefore be able to demonstrate that it has used Client's information only for the purpose for which it was obtained.

6.8 A Regulated Entity should identify and comply with the legal and regulatory requirements applicable to the administration of Client affairs in the jurisdiction(s) in which it conducts business or holds Client assets.

6.9 A Regulated Entity should maintain a documented compliance framework that identifies and tracks the relevant legal and regulatory obligations in each jurisdiction where it conducts business or holds Client assets. This may include internal jurisdictional checklists, reliance on external legal counsel, cross-border compliance protocols, or other recognised industry resources. Where necessary, the Regulated Entity should seek appropriate legal or professional advice to establish that it meets any applicable fiduciary, custodial, or administrative responsibilities under relevant acts and regulations.

6.10 A Regulated Entity must ensure that any decisions made, or transactions entered into by a Client, on behalf of a Client, or in relation to the Client Agreement are: R

(a) within the scope of approval of the Regulated Entity;

(b) documented and actioned by the Regulated Entity in a timely and expeditious manner in accordance with the Client Agreement and commensurate with the size, complexity, structure, nature of business and risk profile of the Client operations; and

(c) properly authorised and handled by persons employed by the Regulated Entity or by the Regulated Entity's Agent with an appropriate level of competence, knowledge, experience, and professional standing.

6.11 With regard to maintaining the timeliness of transactions, a Regulated Entity is guided to transact its business (including establishing, transferring or closing business relationships with its Client) expeditiously, meaning without delay, and in line with the terms of business contained in the Client Agreement. The Regulated Entity should also provide Clients with any information relating to operations on virtual assets that would require a Client's response, without delay.

6.12 A Regulated Entity should inform Clients of the typical timeframes for processing account withdrawals or account closures, including instances where,

due to safeguarding controls (such as virtual assets being stored in offline wallets), virtual asset withdrawals may take longer to process. A Regulated Entity should inform Clients of any withdrawal limits and related timeframes.

6.13 The concept of conflict of interest is generally related to a Regulated Entity putting control activities in place, including segregation of duties, declarations and recusal procedures to mitigate fraud, error or manipulation and to promote integrity, transparency and acting in the best interests of Clients. The Regulated Entity should therefore appropriately segregate the duties of critical functions, including but not limited to Client onboarding, transaction execution, reconciliation, custody, risk monitoring, and compliance.

6.14 The policies and procedures implemented by a Regulated Entity for the identification and management of conflicts of interest should consider:

(a) conflicts of interest between a Regulated Entity and their beneficial owners, directors, senior officers, employees and Clients;

(b) any personal conflicts of interest of any employee tasked with decision-making;

(c) keeping and maintaining a register of potential and existing conflicts of interests, along with the mitigating measures in place; and

(d) avoiding the assignment of conflicting duties to one individual. Certain duties within a Regulated Entity should be split, to the extent possible, among various individuals to reduce the risk of manipulation of financial data or misappropriation of assets.

6.15 A Regulated Entity must disclose any conflict of interest or potential conflict of interest to its Clients; and such disclosure must be in written form and include sufficient detail, taking into account the nature of the Client, to enable the Client to take or make an informed decision with respect to the product or service in the context of which the conflict of interest arises. R

6.16 Every director and senior officer must disclose any conflicts of interest to the Governing Body on at least an annual basis. Where new conflicts arise, directors and senior officers must declare them and recuse themselves from decisions in which a conflict of interest exists. R

6.17 A Regulated Entity must ensure that there is adequate segregation of duties, commensurate with the size, complexity, structure, nature of business and risk profile of its operations. R

6.18 A Regulated Entity must maintain and implement effective policies and procedures to prevent, identify, manage, and disclose conflicts of interest. R

6.19 The Regulated Entity must observe the conflict of interest and confidentiality disclosure requirements outlined in this Rule at all times as an ongoing obligation. R

6.20 Overall, the Authority expects that, throughout the lifetime of the relationship with its Clients, a Regulated Entity maintains appropriate, reliable, timely, and transparent interactions while exercising due care and diligence.

7. Client Asset Safeguards

7.1 A Regulated Entity outsourcing custody of Client virtual assets to third parties must ensure that such third parties are, at all times, in compliance with the relevant requirements under the VASPA, this measure and other applicable regulatory measures. R

7.2 A Regulated Entity holding Client funds, on behalf of Clients, must ensure that Client funds are clearly segregated in compliance with the relevant requirements under the VASPA. R

7.3 Where a Regulated entity decides to cease any virtual asset services, it must ensure that it honours its commitments, protects Client interests, and that any outstanding business is properly completed with minimal disruptions to its clients, and in accordance with the relevant Acts or regulatory measures. R

8. Insurance

8.1 Where applicable, a Regulated Entity must maintain insurance protections to the satisfaction of the Authority, including the following: R

(a) professional liability of senior officers;

(b) theft or loss of Client assets held in custody;

(c) business interruption; and

(d) cyber security.

8.2 Insurance coverage carries an added layer of security, ensuring that Clients are safeguarded against potential losses and can trust the Regulated Entity to act responsibly and transparently. The level of insurance cover that a Regulated Entity holds should be based on the products and services that it offers and its scale of operations. Consideration should be given to the following risks:

(a) loss or theft of virtual assets belonging to Clients;

(b) loss of documents;

(c) misrepresentations or misleading statements made;

(d) acts, errors, or omissions resulting in a breach of:

(i) legal and regulatory obligations;
(ii) the duty to act honestly, fairly, and professionally towards Clients; and
(iii) confidentiality obligations; and

(e) failure to establish, implement and maintain appropriate procedures to prevent conflicts of interest.

8.3 Where a Regulated Entity is unable to obtain such insurance coverage, it should notify the Authority and provide reasonable evidence of unavailability. In such cases, the Authority may permit the use of alternative risk mitigation measures,

taking into account the nature, scale, complexity, and risk profile of the custody services provided. These may include alternatives such as:

(a) Regular independent audits;

(b) Enhanced cybersecurity and operational safeguards; and

(c) Self-funded reserves or risk-based capital (as a form of self-insurance).

All alternative measures would be subject to the approval of the Authority, in advance, and should offer a level of protection broadly equivalent to that of insurance. This exception is not intended to serve as a default alternative to insurance but as a limited accommodation in exceptional cases. Furthermore, the Authority may subject the Regulated Entity to review any self-insurance cover on at least an annual basis, considering the proportionality principle.

9. Marketing, Advertising, Communications, and Promotions

9.1 A Regulated Entity must ensure that all marketing, advertising, or promotional materials and information: R

(a) are fair, clear, and not misleading in both content and presentation;

(b) are clearly identifiable as marketing or promotional in nature;

(c) do not contain statements or visual elements that contradict the risks associated with Virtual Assets;

(d) do not mislead Clients, deliberately or negligently, about the real or perceived benefits of any services carried out, or about potential profitability, exaggerate claims, or make assurances of gains;

(e) do not mislead Clients about the safety, risk profile, simplicity, or guarantee, or create an urgency based on the speculative future value of an investment; or

(f) do not create an urgency based on the speculative future value of an investment.

9.2 A Regulated Entity should ensure that any advertising, marketing, or promotional materials and communications relating to its products or services are fair, clear, and not misleading. In particular, the Regulated Entity should take reasonable steps to ensure that language is carefully chosen and does not include misleading statements, promises, or terms, when read in context, (such as "guaranteed", "confidential", "assured", "secret", or similar expressions), whether relating to the scale of its regulated activities or to any other matter that the Regulated Entity does not reasonably believe to be true. The Regulated Entity should also have regard to the Authority's Policy on Marketing Policies of Licensees.

9.3 A Regulated Entity should establish that all communication and information provided to Clients:

(a) is provided in writing or in a form that can be retained and referenced by the Client. The Authority notes that while typically, a Regulated Entity

communicates with Clients via e-channels, digital channels or applications, the expectation is that the Regulated Entity implements policies and procedures to manage the integrity and auditability of its communication with Clients. This is particularly important to consider, in conjunction with Rule 10.5 and whether such communication impacts the Client Agreement;

(b) uses plain language, is logically ordered, accurate, clear, free of ambiguity and misleading language, technical jargon or complex information that is not clearly explained; highlights important information;

(c) is sufficient for and presented in a way that is likely to be understood by the average Client in the group of Clients to whom it is directed, or by whom it is likely to be received;

(d) does not disguise, diminish or obscure important items, statements or risk warnings, and includes clear, fair and prominent information on the proportion or percentage of Clients that incur losses when trading such products;

(e) uses a font size in the indication of relevant risks that is at least equal to the predominant font size used throughout the information provided, as well as a layout that ensures that such an indication is prominent;

(f) is consistently presented in the same language throughout all forms of information and marketing materials that are provided to each Client, unless the Client has agreed to receive information in more than one language;

(g) is up to date and relevant to the means of communication that the Client has agreed to; and

(h) considers whether the omission of relevant facts would result in the information being unfair and unclear, or misleading.

9.4 Further, the Authority does not require Regulated Entities to make audio or digital screen recordings of telephone calls with Clients. However, where material instructions, advice, or agreements are provided by telephone, Regulated Entities should follow up with written confirmations or follow-up documentation, including the substance of the communication in a durable and auditable format, so as not to breach any obligations relating to the Client agreement.

9.5 While technical or industry-specific terms are not prohibited, Regulated Entities should consider the ways of conveying information, the content that the communication is intended to convey, and the type, experience and level of knowledge and/or sophistication of each Client, to uphold the integrity of such communication. Further, while the Authority does not mandate that Regulated Entities conduct formal tests (for example, quizzes) to assess a Client's level of knowledge and sophistication, Regulated Entities should use reasonable, risk-based evaluation methods considering factors such as product complexity,

Client profile, or onboarding information to tailor communications to Clients appropriately, and with integrity.

9.6 Where a virtual asset service or product carries a lower risk profile based on established technology or operational, or validated history, a Regulated Entity may describe such characteristics in its marketing, advertising or promotion, provided that it does so in a balanced manner that does not diminish disclosure of residual risks.

9.7 A Regulated Entity should not include in its marketing communications any statement detailing historic market performances of its products or services unless:

(a) the basis on which such performance is measured is clearly stated and the presentation is not misleading;

(b) it is accompanied by a risk warning indicating that past performance is not necessarily an indication of future performance; and

(c) the past performance details are relevant to the service or product offered by the Regulated Entity.

9.8 It is also expected that the marketing communications of the Regulated Entity does not compare the products and services to other forms of investments or trading unless the reason for the comparison is clearly stated, justified and appropriate.

9.9 A Regulated Entity must ensure that its marketing, advertising, communications and promotions practices: R

(a) do not breach or contain any material or content that is in breach of any acts, regulations or applicable rules;

(b) do not violate standards of prudence and fairness;

(c) are clear, ethical, factual, and not misleading, false, or deceptive;

(d) do not present or promote any services that it is not licensed or registered or waived to provide;

(e) disclose to its Clients and prospective Clients any material risks that the Regulated Entity, acting with due care and diligence, ought to identify in connection with the virtual asset services it is advertising to them; and

(f) do not place the reputation of the Cayman Islands at risk of being brought into disrepute.

9.10 A Regulated Entity must disclose all incentives and rewards being offered in marketing campaigns, including applicable terms and conditions. R

9.11 The incentives and rewards disclosed should be clearly identified as being offered to the Client. The Regulated Entity should make it clear what the Client will receive, under what conditions, and avoid language that could cause

confusion about whom the reward is intended for.

9.12 Where a Regulated Entity uses a marketing or trading name that differs from its regulated legal name, both names should be clearly disclosed in all marketing, advertising, or promotional materials in a manner that is prominent and not misleading.

9.13 A Regulated Entity should ensure that the marketing of higher risk products, such as derivatives or leveraged trading, includes a warning of the risks involved. These may include:

(a) the enhanced risk of losing invested capital through margin calls or position liquidations;

(b) the impact of small fluctuations in the price of virtual assets;

(c) the risk of imperfect correlation between a derivative and the underlying asset and the resultant hedging risk; and

(d) statistics and statements on the percentage of Clients that lose money when trading with the custodian or trading platform.

9.14 A Regulated Entity should maintain a record of any marketing communications or promotional campaigns. This should be made available to the Authority if necessary.

10. Client Onboarding and Client Agreements

10.1 In assessing the complexity and minimising the risk of its products and services during client onboarding, the Regulated Entity should develop controls, policies and procedures which are proportionate to:

(a) the level of understanding, interest, and needs of its Clients; and

(b) the level of risk, experience, and vulnerability of its Clients.

Examples of measures that a Regulated Entity may take in this regard include *inter alia:*

(a) assessing the volatility and extent to which a product or service is suitable and appropriate for a Client. This may include taking into consideration the nature of the Client (i.e. retail or corporate);

(b) carrying out robust testing of new products and services, and the effectiveness of controls;

(c) considering the extent to which Client assets are at risk as a result of new products or services being offered; and

(d) the Client's risk appetite and financial position.

10.2 The key risks associated with virtual assets products and services, for which risk disclosures or warnings should be made to Clients, include, but are not limited to:

(a) potential loss of value in full or in part or if the Client's invested capital

is at risk;

(b) risks relating to the use of leverage;

(c) the irreversible or illiquid nature of certain transactions;

(d) the absence of financial protection for Virtual Asset investors;

(e) the exposure to fraud, theft, manipulation, or cyber risks;

(f) volatile trading history; and

(g) the risks associated with the transfer and storage of virtual assets, applicable where the Client wishes to deposit or withdraw virtual assets to or from a wallet address controlled by the Regulated Entity.

These disclosures should be presented in a clear, accurate, and easily understandable format across all Client-facing documentation, communications, and agreements.

10.3 Additionally, the Authority notes that all material terms must be fair, transparent, and clearly disclosed to Clients during the onboarding process and in the Client Agreement. This includes, but is not limited to:

(a) terms relating to limitation of liability, indemnification, and the circumstances in which either party may be held liable for losses, damages, or third-party claims; and

(b) any contractual right of a Regulated Entity to realise Clients' virtual assets, including the specific virtual assets subject to that right, the circumstances in which it may be exercised, and the actions the Regulated Entity may take when exercising it.

10.4 Moreover, the Authority notes that terms relating to limitation of liability and indemnification should not be one-sided to an unreasonable extent. For example, indemnities for Client negligence may be acceptable, but not clauses exempting a Regulated Entity from any illicit activity, including fraud or gross negligence.

10.5 A Regulated Entity must ensure that a written Client Agreement is signed by all parties and in place before providing any virtual asset service(s) under the VASPA and must provide the Client with a copy of the executed Client Agreement. R

10.6 A Regulated Entity must clearly specify in the Client Agreement the nature of each service or product it provides to the Client, as well as the capacity in which it acts in relation to any relevant transaction. R

10.7 The Regulated Entity must clearly identify all parties to the Client Agreement, including the legal name and registered address of the Regulated Entity, and, where applicable, any affiliated or parent entities, or provisions for custodial or other third-party arrangements that are materially connected to the provision of the virtual asset services. The Regulated Entity must also correctly identify the Client by legal name, and, where applicable, any additional party authorised to act on the Client's behalf. R

10.8 A Regulated Entity must clearly disclose, in the Client Agreement/ Terms of business / other relevant documents and in a manner that is simple and easy for the Client to understand, the quantity, value, and arrangements for the payment or provision of any commissions, fees, interest, charges, inducements, or other costs associated with the provision of virtual asset services, together with any applicable terms and conditions. The fees, charges or commission structures must be transparent, fair, and non-discriminatory. R

10.9 The written Client Agreement should be shared between the Regulated Entity and the Client via a suitable documented communication method, such as email, smart contract, or secure Client portal access. The Authority expects that such Client Agreement is recorded, captured, or stored in a manner that ensures it can be accessed and verified by the Authority.

10.10 A Regulated Entity must provide Clients with written confirmation upon execution of a transaction that includes all relevant details of the transaction. R

10.11 The Regulated Entity should also consider providing written confirmation to the Client on the following:

(a) the virtual asset being transacted along with the price, quantity and total cost;

(b) the date and time that the transaction was placed;

(c) in relation to the transaction details, if applicable, the direction of the transaction (e.g. buy or sell order);

(d) the allocation and provision of an order identification number so that the Client will be able to communicate with the Regulated Entity in the event of any discrepancies, operational issues, or complaints; and

(e) providing any funds, commission, or fees received in connection with any Client transaction.

10.12 The executed Client Agreement and written confirmation of a transaction, including the transaction details, may be provided to the Client in secure Client portals, via email, or other reliable and auditable electronic means.

10.13 A Regulated Entity should also consider including within the Client Agreement the manner in which the Client may provide instructions for any transactions. Generally, it should be established that the Client Agreement includes clear and accurate information on the official Communication Channels used between the Regulated Entity and the Client. This guidance supports Client awareness, reduces confusion, and aims to protect Clients from fraud, impersonation, scams or similar threats.

10.14 The Regulated Entity must include a dedicated section in the Client Agreement/ Terms and Conditions/ or an Alternative that prominently discloses all key risks associated with the virtual assets provided and written in plain language to ensure that Clients are aware of, and have acknowledged such risks, and can make well-informed decisions about engaging in the virtual asset service (s). R

Disclosures of key risks in the Client Agreement / Terms and Conditions/ or an Alternative must be assessed and updated to reflect evolving risks.

10.15 The Regulated Entity must disclose in the Client Agreement and other relevant documents, internal safeguards that it has implemented to mitigate key risks, including, where applicable, the methods of access to virtual assets held and insurance arrangements for the protection of these assets. R

10.16 A Regulated Entity must always comply with the terms and conditions of the Client Agreement, unless otherwise required by law or waived with Client consent. R

10.17 Where a waiver from the terms of the Client Agreement is granted, the Regulated Entity should document and retain evidence of the Client's consent and the basis for the waiver. Such records should be maintained in accordance with the entity's record-keeping policies and be made available to the Authority upon request.

10.18 A Regulated Entity must provide prior written disclosure of any amendments that it intends to make to the Client Agreement/ Terms of business, and the manner in which the amendments can be made, and any associated or indirect costs, allowing a reasonable opportunity for the Client to accept, reject, or terminate the Client Agreement without any penalties, other than for the settlement of any outstanding obligations or liabilities under the Client Agreement. R

10.19 Such amendments to the Client Agreement may include, but are not limited to, changes to fees, commissions, the structure of the business, conflicts of interest, changes in management, and control functions. Following the provision of such notice disclosure of any amendment to the Client, a Regulated Entity should clearly state that continued use of its virtual asset services will constitute acceptance of the amended terms of the Client Agreement. This approach reflects common commercial practice, provided Clients are given adequate notice and a fair opportunity to terminate without penalty.

10.20 The Regulated Entity must ensure that: R

(a) it has obtained and documented all relevant information about the Client's objectives, financial situation, risk tolerance, knowledge, experience and the understanding of the risks involved; and any other factors necessary to make an informed and appropriate decision on the Client's behalf;

(b) the products and services offered to each Client are suitable, having regard to the factors in (a) in the above;

(c) the discretion or power given to it, is used for proper purpose, in the Client's best interests, and in line with the Client Agreement; and

(d) there is documented evidence to record decisions made under discretion, where the Regulated Entity has been granted discretion to act on behalf of Client.

10.21 The Authority expects that dispute resolution mechanisms available to a Client, including escalation pathways and resolution timelines, are also clearly defined in a Client Agreement.

10.22 A Regulated Entity should consider informing Clients within the Client Agreement / terms and conditions or an alternative of the regulated activity that it performs, the jurisdiction(s) and those who are responsible for regulating it.

10.23 When structuring the Client Agreement, the Regulated Entity should include the arrangements for bringing the Client Agreement to an end.

11. Complaints Handling

11.1 A Regulated Entity must establish effective complaints-handling policies and procedures that ensure fair, consistent, and impartial management of complaints. R

11.2 The complaints-handling framework should be disclosed in a clear and easy-to-understand manner to establish accessibility and transparency for Clients, including by providing a standardised template or other simple method that enables any Client to submit a complaint easily. A Regulated Entity may disclose this information through its website or other communication channels, including social media platforms.

11.3 Upon receipt of a complaint, a Regulated Entity must, without delay, acknowledge the complaint in writing and inform the complainant that it is being considered. R

11.4 The Regulated Entity must investigate and address Client complaints in a timely, fair and consistent manner and communicate the outcome of the complaints within a reasonable timeframe. R

11.5 The Regulated Entity must maintain a log of Client complaints and resolutions for operational risk management purposes, which must be made available to the Authority upon request. This log must meet record-keeping requirements in relation to all Client complaints and resolutions, including: R

(a) details of each complaint;

(b) date received;

(c) response and actions taken;

(d) Status of the complaint (whether resolved/unresolved), complaints; and

(e) date resolved.

11.6 The Regulated Entity must report to the Authority any Client complaint or a set of Client complaints that represent a material risk to Clients or are indicative of a material failure of the Regulated Entity's control environment. R

11.7 Pursuant to the Anti-Money Laundering Regulations, a Regulated Entity is mandated to keep records for a minimum of five (5) years, from the date of

resolution. Where a longer retention period is necessary due to the nature of the complaint, legal risk, or internal policy, the Authority expects that Regulated Entities retain such records for up to seven (7) years or more, in line with best international practices and internal governance requirements.

11.8 The Regulated Entity should provide the Governing Body with regular reports on complaints handling, including sufficient analyses of complaint trends, all ongoing complaints data, outcomes and any potential systemic issues. This aims to promote proper oversight of the complaints handling programme on an ongoing basis, to identify patterns about the issues, and implement corrective measures to avoid recurrence.

11.9 A Regulated Entity is expected to maintain procedures and systems that keep complainants informed of the progress of their complaint through proactive written updates. These procedures and systems should, at a minimum, require written acknowledgement of receipt of a complaint and set clear expectations for update timelines that are appropriate to the nature and complexity of the complaint.

11.10 A Regulated Entity should openly communicate the details of the status of the resolution to the complainant within a reasonable timeframe, such as:

(a) the alternative resolution options, irrespective of whether or not the complaint is resolved in a manner that they are satisfied with;

(b) whether the complaint needs to be escalated for further enquiry; and

(c) expected timeframe for the complaint to eventually be resolved.

This is particularly more important in cases where the complaint is complex or uncommon in nature. Communication should remain consistent with any applicable legal restrictions.

11.11 A Regulated Entity should confirm to the Complainant in writing when a complaint has been closed.

11.12 If a Regulated Entity concludes that it is not upholding a complaint, it should communicate this to the complainant in writing, clearly stating the reason(s) for its decision in accordance with the Regulated Entity's relevant policies or evidence, to establish transparency and to help the complainant understand the rationale.

11.13 Where the provision of virtual asset services involves an Agent, a Regulated Entity must establish procedures to facilitate the handling of complaints between its Clients and such Agents. R

11.14 Notwithstanding the involvement of an Agent, the Regulated Entity remains fully responsible for the resolution of all Client complaints.

11.15 A Regulated Entity must not impose any fees or charges on Clients for the submission or handling of complaints. R

12. Public Disclosures

12.1 A Regulated Entity must make public disclosures readily available across all Communication Channels as appropriate, and present them in a manner that is clear, concise, and easy to understand. R

12.2 In respect of Rule 12.1 above, Public Disclosures include but are not limited to the disclosures about organisational changes, service or product offerings, risk factors, fees or changes in fees (as applicable), and regulatory status. Additionally, disclosures should be made in a manner that is easily accessible and understandable across the communication channels.

12.3 A Regulated Entity should publicly disclose its licensing or registration status and authorised number, as approved by the Authority.

12.4 A Regulated Entity must publish information related to its key corporate governance structures, as well as the identification and details of the members of its Governing Body, Control Functions and Senior Management. R

12.5 When disclosing information on governance structures, a Regulated Entity should do so in a manner consistent with applicable data privacy laws. Disclosure does not extend to personal data such as home addresses or other sensitive information. Instead, the Authority expects publication of information, including, but not limited to, the person's name, title/role, and professional designation. These disclosures assure competence, knowledge, and professionalism, consistent with the obligations set out in Rule 6.10(c) on Integrity.

12.6 Pursuant to the relevant Acts, a Regulated Entity should report material changes in its operations to the Authority where such changes are reasonably expected to significantly impact Clients' interests, regulatory compliance, or the Regulated Entity's risk profile. In the same vein, the Regulated Entity should consider whether to disclose such material changes to its Clients to avoid breaching Rules 12.1 or 12.4.

12.7 Material changes in a Regulated Entity's operation include, but are not limited to, the following occurrences:

(a) breaches of security or significant operational changes;

(b) any significant alteration to a VASP's operations or structure;

(c) offerings that could impact Clients, stakeholders, or regulatory compliance;

(d) service disruptions;

(e) modifications to terms of service or fees;

(f) shifts in ownership or management; and

(g) sale or cessation of the Regulated Entity's operations.

12.8 If a Regulated Entity engages or partners with a third-party service provider in connection with the obligation of its services (for example, a bank that holds fiat funds), it should clearly disclose to its Clients the nature of the arrangement

and identify the party with whom the Client is transacting.

12.9 Where a Regulated Entity is part of a larger group structure, Clients should be made aware of which group entity they are transacting with at all times, including the regulatory status of that entity, and the level of protection afforded to the Client.

12.10 Where a Regulated Entity decides to cease any virtual asset services, it must notify the Authority and provide a plan for communicating its cessation to stakeholders for the Authority's approval. R

13. Cross-Border Transactions

13.1 Regulated Entities should align their cross-border transaction practices with international standards, including the FATF Recommendations related to virtual assets and virtual asset service providers.

13.2 A Regulated Entity should notify the Client of the required information for cross-border transactions, including transaction identifiers.

13.3 As a best practice, all fees associated with cross-border transactions, including conversion costs and transmission charges, should be disclosed in advance.

13.4 A Regulated Entity should establish that its Clients are informed in real time whenever material updates arise regarding the status of cross-border transactions. Any delays or issues affecting cross-border transactions should be communicated to the affected Client without delay.

14. Trading on Own Account

14.1 Proprietary trades should be executed under the same conditions as Client trades to establish fairness.

14.2 A Regulated Entity must implement and maintain effective systems, controls, and procedures to prevent market manipulation, insider trading, and other abusive trading practices in connection with its proprietary trading activities. R

14.3 Such systems, controls, and procedures should apply to all proprietary trading activities, whether conducted on-platform or off-platform. The systems, controls and procedures include, but are not limited to:

(a) Real-time surveillance capable of detecting abusive practices such as spoofing, layering, wash trading, front-running, and insider trading;

(b) Automated alerting tools and data retention systems to support forensic analysis;

(c) Documented escalation protocols and internal reporting for suspicious or cancelled orders;

(d) Regular internal reviews and, where appropriate, independent audits of the effectiveness of controls;

(e) Governance arrangements that clearly assign accountability for surveillance and order handling; and

(f) Information barriers and trade handling rules to establish a clear separation between proprietary and Client-facing activities.

Additionally, the Authority expects these systems, controls, and procedures to be commensurate with the Regulated Entity's size, complexity, and risk profile, and to include appropriate audit trails and escalation mechanisms.

14.4 Proprietary trading must not compromise trading conditions or create unfair trading advantages. R

14.5 A Regulated Entity should establish that its proprietary trading activities are subject to appropriate internal controls, including but not limited to:

(a) information barriers between proprietary and Client-facing functions;

(b) fair and non-preferential access to liquidity and order execution; and

(c) Continuous monitoring to detect and prevent conflicts of interest or preferential treatment.

These controls help to ensure that Client orders are not disadvantaged and that the Regulated Entity acts in accordance with the principle of market fairness.

14.6 A Regulated Entity should establish that the internal controls outlined in 14.5 are supported by documented policies and procedures, including but not limited to:

(a) governance arrangements that establish accountability for oversight of proprietary and Client-facing activities;

(b) clearly defined procedures to identify, manage, and escalate conflicts of interest;

(c) control mechanisms to establish order execution practices that do not favour proprietary trades over Client orders; and

(d) periodic assessment of the effectiveness of information barriers and access controls.

14.7 A Regulated Entity must not use Client data to gain an unfair advantage in trading activities, including its proprietary trading. R

14.8 To prevent such misuse and remain consistent with the Authority's expectations for market conduct and Client protection, a Regulated Entity should implement appropriate safeguards, including but not limited to:

(a) Information barriers between proprietary and Client-facing functions, supported by system-level access controls and audit trails;

(b) Independent surveillance functions with the authority to monitor internal and third-party data access; and

(c) Maintenance of auditable records of how Client data is accessed, used, and protected.

All use of Client data should remain consistent with the Authority's expectations for market conduct and Client protection.

14.9 Client data includes, but is not limited to, a Client's trade history, open or historical bid/ask positions, order book interactions, trading frequency, behavioural patterns, and any other transaction-related data or metadata that could inform or influence a Regulated Entity's trading strategy. Such data should not be accessed or used by proprietary trading teams unless it has been sufficiently anonymised and aggregated, and only where:

(a) Its use is demonstrably in the Client's best interest, such as for suitability assessments; or

(b) The Client has provided explicit, informed consent.

All access to Client data should comply with the requirements set out in Rule 14.7.

B. Additional Rules and Guidelines Relating to Virtual Asset Trading Platforms and Virtual Asset Custodians

15. Virtual Asset Trading Platforms

15.1 VATPs must implement systems and procedures to monitor, detect and prevent suspicious transactions, market abuse, and promote the best interests of Clients and the integrity of the market. R

15.2 A VATP must undertake regular assessments to identify the inherent risks associated with market abuses, such as insider dealing and market manipulation, and determine the necessary measures to mitigate these risks. R

15.3 VATPs must immediately report to the Authority any suspicions indicating that market abuse or other unfair trading practices are being, have been, or are likely to be committed. R

15.4 VATPs should implement appropriate surveillance arrangements that apply to all virtual asset product offerings and should at least annually reconcile the coverage of such arrangements against their risk assessment.

15.5 The VATPs market abuse surveillance framework, whether manual or automated, should be established appropriately to the size, nature, and complexity of the VATP. Consideration should be given to:

(a) the number of transactions that will need to be monitored;

(b) the type of virtual asset being traded by the Client;

(c) the frequency and volume of orders and transactions; and

(d) the risk profile of the VATP.

15.6 The VATPs market abuse surveillance framework should include procedures, measures, and systems that detect wrongdoings such as insider trading or market manipulation. For the framework to be comprehensive, proactive, and practical, it should comprise of systems designed to monitor trading patterns, detect suspicious activities, and ensure that adequate actions are taken to prevent market manipulation.

15.7 VATPs should maintain a publicly accessible interface, such as a dashboard, displaying key market metrics like market trends, trade volumes, and other relevant data. This information should be presented in an easily understandable and user-friendly format, such as graphs, charts, or tables, to establish that users can access and interpret market data effectively.

15.8 A VATP should establish and maintain systems, policies, and procedures for the proper handling and protection of material non-public information ("MNPI"), including, where applicable, information related to whether a virtual asset will be admitted or listed for trading on its VATP. MNPI includes any non-public data that, if disclosed, could influence a decision to buy, sell, or hold a virtual asset. This includes, but is not limited to, information about planned listings, de-listings, major upgrades, partnerships, or technical vulnerabilities. The VATP should take proactive measures to prevent the leaking or misuse of such information.

15.9 VATPs must make their pricing policies, including information on price discovery mechanisms, such as live pricing, real-time bid-ask spreads, and transaction fees, easily accessible and publicly available and prominently and clearly displayed on their website, platform, or any other medium used to provide access to their virtual asset services. R

15.10 A VATP must implement pricing policies and procedures that prevent unfair trading activities and market abuse. R

15.11 The VATP should implement effective system controls to reject transactions that would exceed the internal volume and price thresholds.

15.12 A VATP should have policies and procedures in place for analysing, individually or comparatively, each transaction executed and order priced, modified, cancelled, or rejected in its system.

15.13 For the purposes of Rules 15.9 and 15.10 above, VATPs should ensure that pricing information is continuously updated to reflect prevailing market conditions in real time. Where feasible, VATPs should enable Clients to access or be redirected to the original source(s) or the breakdown of pricing components used to compile the displayed pricing data, such as interchange rates and fees for each product and service provided. To prevent price manipulation and any unfair trading practices, price discovery methods should therefore include pre-trade and post-trade transparency, relating to the bid and offer prices, the depth of trading interests on prices advertised on trading platforms, and volume and transaction times. Overall, these measures aim to enhance transparency and support Clients in making informed decisions.

15.14 A VATP must disclose fee structures, including all applicable charges, upfront before the execution of any transaction. R

15.15 VATPs must provide real-time order book data, showing aggregated buy and sell orders to Clients as appropriate, while maintaining confidentiality for sensitive information. R

15.16 The Authority expects that the VATPs establish that the real-time order book displays only non-sensitive data, such as aggregated order volumes, across all Communication Channels, while protecting individual order details, user identities, and any other private or proprietary trading information from being exposed to unauthorised parties.

15.17 A VATP must ensure the timely and consistent reconciliation of Client asset balances at suitable, frequent intervals to ensure that Clients' account balances or positions are accurate and provide Clients with applicable verification mechanisms R

16. Virtual Asset Custodians

16.1 A Virtual Asset Custodian must ensure that Client assets are clearly identified and segregated from the proprietary assets of the Regulated Entity as well as assets of its group entities. R

16.2 A Virtual Asset Custodian must ensure that virtual assets and fiat funds belonging to Clients are protected from third-party creditors. R

16.3 For the purposes of Rule 16.1 and 16.2 above, segregation should include clear operational and legal separation of Client assets from those of the Regulated Entity and its group entities. Where shared wallet infrastructure or global systems are used, the Regulated Entity should demonstrate that Client assets attributable to its Cayman operations are clearly identifiable, auditable, and not exposed to claims by creditors of the Regulated Entity. Transaction fees initially received into Client wallets should be swept into proprietary wallets on a frequent and auditable basis. Where a global pooled order book is used, the Regulated Entity should ensure that Clients are afforded fair access, competitive pricing, and appropriate disclosures in line with the Authority's expectations regarding market conduct and transparency.

16.4 A Virtual Asset Custodian must establish a custody policy with internal rules and procedures to ensure the safekeeping and control of virtual assets in its custody, as well as the means of access to them. R

16.5 A Virtual Asset Custodian must ensure that any economic, governance, or other benefits arising from the custody of a Client's virtual assets, including, but not limited to, staking rewards, airdrops, or voting rights, are treated in accordance with the terms agreed with the Client. The Virtual Asset Custodian must clearly disclose the nature of such benefits to the Client and obtain the Client's consent regarding their retention, application, or transfer. R

16.6 A Virtual Asset Custodian must implement robust security measures to protect Client assets. R

16.7 For the purposes of Rule 16.6, robust security measures include the following, *inter alia*:

(a) multi-factor authentication and access controls;

(b) secure key management protocols (e.g., management of public and private keys or other related methods by which virtual assets are held,

or multi-signature or hardware security modules);

(c) ongoing threat monitoring and intrusion detection;

(d) recurring testing of IT security and access management; periodic penetration testing; independent third-party security assessments; and

(e) business continuity and incident response plans.

The Regulated Entity should maintain internal documentation to support the effectiveness of these measures, such as audits and relevant accreditations, and should make such documentation available to the Authority upon request.

16.8 A Regulated Entity that provides virtual asset custody services should ensure that it adheres to the latest industry standards in relation to the use of online and offline wallets and implements appropriate security and cybersecurity controls to safeguard Client assets from unauthorised access, fraud, or theft. Such measures may include, but are not limited to, regular and secure backup systems, wallet software updates, robust cybersecurity controls, delegated limits of authority, and other equivalent technical or operational safeguards.

16.9 A Virtual Asset Custodian must provide the Client with clear and accurate information on storage methods used for their virtual assets. R

16.10 A Virtual Asset Custodian should provide Clients with clear information on storage methods (e.g., hot, cold, or other secure storage) and the associated benefits, risks, and security features. The Virtual Asset Custodian should:

(a) provide at least quarterly an update summarising its current storage posture (including indicative allocation across storage methods) and confirm whether there have been material changes since the prior update (a "no material changes" statement is acceptable where applicable); and

(b) promptly notify Clients of any material change to storage methods or infrastructure when it occurs, particularly where risk may increase.

16.11 A Virtual Asset Custodian must report any breaches or unauthorised access to custody systems to the Authority and the affected Clients. R

16.12 For the purposes of Rule 16.11, a Regulated Entity should report any material breach or unauthorised access to its custody systems in a timely manner that upholds Client protection, facilitates effective regulatory oversight, and preserves market integrity:

(a) notification to the Authority: A Regulated Entity should notify the Authority no later than 72 hours after discovery of a material incident, as prescribed under the *Authority's Rule and Statement of Guidance on Cybersecurity for Regulated Entities*.

(b) notification to Clients: In the same vein, affected Clients should be notified promptly after notification to the Authority, once the nature and impact of the breach has been reasonably assessed, and in any event no later than 72 hours from detection, unless otherwise directed by

investigative or regulatory authorities.

(c) recordkeeping: All incidents, whether material or not, should be documented internally, including the timeline of detection, actions taken, and any reasons for delay in reporting. These records should be made available to the Authority upon request.

16.13 A Virtual Asset Custodian must ensure the timely and consistent reconciliation of Client asset balances at suitable, frequent intervals to ensure that Clients' account balances or positions are accurate. The Virtual Asset Custodian must also provide Clients with applicable mechanisms to verify their balances or positions. R

16.14 With regards to the reconciliation of Client asset balances, a Virtual Asset Custodian must maintain a register of the positions in the name of each Client, including, but not limited to, the following: R

(a) the value and the Client ownership of the virtual assets;

(b) the ongoing record of any movement in the Client positions;

(c) evidence of corresponding transactions;

(d) the frequency of performing the reconciliation of Client virtual assets balances and fiat balances; and

(e) reconciling internally calculated balances to the expected balance on the relevant distributed ledger; investigating any discrepancies; and taking the necessary measures to remedy any differences.

16.15 Reconciliation and verification mechanisms may be automated, comprising a secure and auditable process that enables a Client to confirm the existence and accuracy of their custodied asset balances, which are applied to correct wallet addresses without undue delay, without compromising the security or confidentiality of other Clients. Acceptable mechanisms may include, but are not limited to:

(a) Secure Client account statements or read-only portals; and

(b) Access to On-chain or tagged wallet addresses.

16.16 The reconciliations should be conducted at intervals appropriate to the nature and scale of the custody services, and, for further guidance, should include, at a minimum, daily reconciliation of the account balances of the Virtual Asset Custodian's own assets and of virtual assets and fiat funds belonging to clients. Documentation of the reconciliation should be retained and made available to the Authority upon request.

17. Enforcement

17.1 A Regulated Entity must observe all requirements and expectations within this Rule and Statement of Guidance on an ongoing basis and must not circumvent or attempt to circumvent the requirements contained herein. R

17.2 Whenever there has been a breach of the Rules included in this document, the Authority's policies and procedures, as contained in its Enforcement Manual, will apply in addition to any other powers provided in the relevant Acts and the MAA.

18. Effective Date

18.1 This RSOG will take effect upon **publication in the Gazette**.

Pavilion East, Cricket Square
PO Box 10052
Grand Cayman KY1-1001
Cayman Islands

Tel: +1 (345) 949-7089
www.cima.ky