39-43 Barbados Avenue | Kingston 5, Jamaica W.I.
Telephone: (876) 906-3010 | www.fscjamaica.org

FOR CONSULTATION

PROPOSED BUSINESS CONDUCT STANDARDS

For Virtual Asset Service Providers

List of Acronyms

Acronym	Meaning
Act	Virtual Asset Service Providers Act (proposed)
AML/CFT	Anti-Money Laundering / Combating the Financing of Terrorism
FATF	Financial Action Task Force
FSC / Commission	Financial Services Commission
GDPA	Data Protection Act
VA	Virtual Asset
VASP	Virtual Asset Service Provider
VATP	Virtual Asset Trading Platform

APPENDIX II – PROPOSED BUSINESS CONDUCT STANDARDS FOR VASPs

1. Introduction

1. This document establishes the Financial Services Commission's (the "Commission" or "FSC") proposed Business Conduct Standards for Virtual Asset Service Providers ("VASPs"). It sets out supervisory standards and expectations governing the conduct of VASPs providing virtual asset services to persons located in Jamaica, whether from within Jamaica or from elsewhere, pursuant to the proposed Virtual Asset Service Providers Act (the " VASP Act"). These standards should be read alongside the relevant legislation, regulations, and any other supervisory rules or guidance issued by the Commission in relation to VASPs.

2. Purpose

2. The purpose is to establish minimum business conduct standards applicable to all VASPs licensed by the Commission under the proposed VASP Act. These standards are intended to promote:
    - fair, transparent, and responsible conduct in the provision of virtual asset services;
    - the protection of clients and market participants;
    - the integrity and orderly functioning of virtual asset markets; and
    - sound governance and risk management practices within VASPs.
3. In establishing these standards, the Commission seeks to ensure that VASPs operate in a manner consistent with the regulatory objectives of consumer protection, market integrity, and the safe and responsible operation of the virtual asset sector in Jamaica.

4. Scope of Application

4. This applies to all licensees under the Act, including entities engaged in:
    - the operation of virtual asset trading platforms;
    - brokerage or dealing in virtual assets;
    - the provision of virtual asset custody services;
    - virtual asset advisory services;
    - virtual asset wallet services; and
    - virtual asset conversion or exchange services.
5. The standards apply to the conduct of VASPs in relation to their operations, internal governance arrangements, and dealings with clients, counterparties, and the Commission. The FSC adopts a risk-based and proportionate approach in applying these stndards, taking into account the nature, scale, complexity, and risk profile of each VASP's operations. The Commission may issue supplementary guidance applicable to particular licensees.

5. Definitions

6. For the purposes of this document:
    - "client" or "customer" means a legal or natural person to whom virtual asset services are provided.

- "cross-border transaction" refers to any transaction in which the originator and beneficiary are in different jurisdictions, including any series of transactions involving at least one cross-border element.
- "officer" has the same meaning as defined in the proposed VASP Act.
- "senior management" means the persons responsible for the day-to-day management of the VASP's operations, including the compliance and risk management functions.
- All other terms carry the meanings given in the Act or in the FSC AML/CFT/CPF Guidelines, as applicable.

6. High-Level Guiding Principles

7. The following principles underpin the specific conduct standards set out in Section 7 and inform the Commission's approach to supervisory assessment.

Principle	Description
Honesty and Integrity	VASPs must conduct their operations and communications in an honest and ethical manner and must not pose a risk to the public or to the reputation of Jamaica.
Fair Treatment of Clients	VASPs must pay due regard to the interests of their clients and treat them fairly. All communications must be accurate, comprehensible, and appropriate to the client.
Protection of Client Data	VASPs must protect client personal data through adequate storage, data protection, maintenance, and record-keeping in compliance with the Data Protection Act, 2020.
Protection and Segregation of Client Assets	VASPs must take all steps to protect client assets and ensure they are clearly identified and segregated from the VASP's proprietary assets at all times.
Maintenance of Security Systems	VASPs must maintain appropriate systems and security protocols to guard effectively against cyber threats. All staff, including the board and senior management, must be aware of relevant cybersecurity risks.
Due Skill, Care and Diligence	VASPs must conduct business with due skill, care, and diligence; employ forward-looking risk management; and continuously consider risks to clients and the reputation of Jamaica.
Prevention of Financial Crime	VASPs must have appropriate systems, policies, and procedures to ensure compliance with all applicable AML/CFT legislation.
Management of Conflicts of Interest	VASPs must identify and effectively manage conflicts of interest and put in place mechanisms to prevent market manipulation, collusion, and front-running.
Adequate Resources	VASPs must maintain adequate financial and non-financial resources — including sufficient capital and appropriate insurance — commensurate with the size, scope, and complexity of their business.

Principle	Description
Full Disclosure	VASPs must provide full and proper disclosure of their operations, including the capacity in which they act, risks associated with custodial arrangements or investments, and the amount or arrangements for payment of commissions or other inducements.
Corporate Governance and Resilience	VASPs must maintain effective corporate governance arrangements and robust contingency planning to ensure minimal disruption to clients in all circumstances, including in the event of wind-down.
Regulatory Compliance	VASPs must continuously assess their operations and management systems to ensure ongoing compliance with applicable laws and regulations in Jamaica.

7. Business Conduct Standards

7.1 Corporate Governance

8. A VASP must maintain a governance framework commensurate with the nature, scale, and complexity of its operations. The board of directors bears ultimate responsibility for compliance with applicable laws and regulatory requirements. At minimum, governance arrangements must include:
    - clearly defined roles and responsibilities for the board, senior management, and key functions;
    - an adequate number of directors with collective skills sufficient to provide effective oversight;
    - board-approved policies covering risk management, internal controls, compliance, and business conduct;
    - an independent compliance function with direct reporting lines to the board or a designated board committee;
    - an internal audit or review function to assess the effectiveness of the control environment;
    - documented succession planning and delegation arrangements for key roles; and
    - board meeting procedures including minimum frequency, quorum requirements, and minute-keeping.
9. The board must review and approve the VASP's risk appetite and risk management framework at least annually and must ensure senior management implements approved risk management strategies.

7.2 Marketing, Promotions, and Communications

10. All marketing, promotional, and client-facing communications must be: fair, clear, and not misleading; accurate and consistent with the VASP's actual services and capabilities; presented in a form the intended recipient can reasonably be expected to understand; free from misleading representations concerning potential returns, risks, or regulatory status; and compliant with applicable consumer protection legislation. Risk warnings must be prominent and must not be obscured by other content. VASPs must not make representations that overstate the security of client assets or understate material risks.

7.3 Client Onboarding

11. VASPs must maintain documented client onboarding policies and procedures ensuring: identification and verification of client identity prior to commencing any virtual asset service relationship, in accordance with applicable AML/CFT requirements; assessment of the client's experience and understanding of virtual assets where relevant to the services to be provided; disclosure of the full terms and conditions, fees, risks, and limitations prior to onboarding; maintenance of accurate and up-to-date client records; and a clear process for client offboarding, including the return or transfer of client assets. Digital onboarding must provide safeguards equivalent to in-person procedures.

7.4 Safeguard of Client Assets

12. VASPs holding or controlling client virtual assets or fiat currency must ensure those assets are adequately safeguarded at all times. Minimum requirements include:
    - clear segregation between client assets and the VASP's own assets — commingling is prohibited;
    - accurate and complete records of each client's assets, capable of immediate reconciliation;
    - holding of client assets in a manner that protects them from the VASP's insolvency;
    - disclosure to clients of how their assets are held, associated risks, and applicable insurance coverage;
    - insurance or equivalent protections covering client asset loss from theft, hacking, fraud, or other unforeseen events; and
    - regular internal reconciliation and periodic independent audit of client asset holdings.

13. VASPs must not use client assets for their own account, proprietary trading, or as collateral for the VASP's obligations without the client's explicit, informed written consent.

7.5 Market Manipulation

14. VASPs must not engage in, facilitate, or permit market manipulation in relation to any virtual asset or market. VASPs must have in place systems, controls, and surveillance capabilities to detect, prevent, and report manipulative behaviour. Prohibited practices include:
    - wash trading — entering into transactions to create artificial trading volume or the appearance of market activity;
    - pump-and-dump schemes — artificially inflating a virtual asset's price before selling at the inflated price;
    - spoofing and layering — placing and cancelling orders with no intention of execution to create a false impression of supply or demand;
    - oracle manipulation — deliberately manipulating data sources used to determine virtual asset prices in DeFi protocols;
    - front-running — exploiting advance knowledge of pending client orders to trade for the VASP's own account; and
    - any other practice that distorts the price or liquidity of a virtual asset or market.

15. VASPs must report suspected market manipulation by clients or counterparties to the FSC promptly.

7.6 Conflict of Interest

16. VASPs must identify, manage, and mitigate conflicts of interest arising from their business activities. VASPs must: maintain a board-approved conflicts of interest policy; identify and record all actual and potential conflicts; implement controls to prevent conflicts from adversely affecting clients; disclose material conflicts to clients where they cannot be adequately managed otherwise; and review the policy at least annually. VASPs must not permit conflicts to compromise the objectivity of client advice, execution of client orders, or fairness of market activity.

7.7 Outsourcing and Third-Party Relationships

17. VASPs may outsource certain operational functions provided outsourcing does not impair their ability to meet regulatory obligations or the FSC's ability to supervise effectively. VASPs must: conduct due diligence on all third-party service providers; enter into documented service agreements assigning responsibility for regulatory compliance; maintain oversight of third-party performance; ensure the FSC has access to information held by third parties on the VASP's behalf; and notify the FSC of any material outsourcing arrangements and significant failures or changes. The outsourcing of a function does not transfer the VASP's regulatory responsibility, i.e. the VASP remains fully accountable for the acts and omissions of its outsourced providers.

7.8 Public Disclosures

18. VASPs must maintain a publicly accessible disclosure — on their website or another accessible channel — providing accurate and current information on: the VASP's licence status and licence number; categories of services authorised; principal risks associated with services; applicable fees, charges, and spread policies; how client assets are held and applicable insurance coverage; the complaints handling process; and any material conflicts of interest not otherwise managed. Disclosures must be updated promptly to reflect material changes. VASPs must not misrepresent their regulatory status or scope of authorisation in any public-facing material.

7.9 Complaints Handling and Dispute Resolution

19. VASPs must maintain a board-approved documented complaints handling policy ensuring: acknowledgement of all client complaints within five (5) business days of receipt; investigation and resolution within thirty (30) business days in ordinary circumstances; ongoing communication to clients on complaint status and outcome; maintenance of a complete complaints register recording the nature and outcome of each complaint; and escalation of systemic issues to senior management and the board. VASPs must not discourage clients from making complaints. A complaints summary report must be submitted to the FSC at the frequency specified in supplementary guidance.

7.10 Insurance

20. VASPs must maintain adequate insurance covering at minimum: theft or misappropriation of virtual assets held on behalf of clients; hacking, cybersecurity incidents, or technology failures resulting in asset loss; and fraud by employees or directors. VASPs must disclose the nature and extent of insurance coverage to clients. The Commission may issue supplementary guidance specifying minimum insurance levels or types of coverage required.

7.11 Data Protection

21. VASPs must handle all client and counterparty personal data in compliance with the Data Protection Act, 2020 and regulations thereunder. VASPs must: maintain a board-approved data protection policy; appoint a data protection officer or equivalent responsible person; implement technical and organisational measures to protect personal data against unauthorised access, loss, or disclosure; inform clients about data collection, use, and retention; and notify the Office of the Information Commissioner and affected clients of any data breach in accordance with applicable requirements. VASPs must not use client data for purposes beyond those for which it was collected without the client's informed consent.

7.12 Cross-Border Transactions

22. VASPs engaging in or facilitating cross-border virtual asset transactions must: assess and manage additional ML/TF/PF risks in line with applicable AML/CFT requirements; ensure compliance with the Travel Rule as set out in the VASP AML/CFT/CPF Guidelines; assess the regulatory status of counterpart VASPs and apply enhanced due diligence where the counterpart operates in a jurisdiction with inadequate AML/CFT controls; and maintain records of cross-border transactions as required under applicable legislation.

7.13 Virtual Asset Trading Platforms

23. VASPs operating virtual asset trading platforms must, in addition to the general standards in this Supervisory Rule:
    - maintain fair, transparent, and non-discriminatory access for all eligible participants;
    - maintain documented and publicly available trading rules, fee structures, and order matching procedures;
    - implement surveillance systems capable of detecting market manipulation and abusive trading practices in real or near-real time;
    - maintain records of all orders and executed transactions — including timestamp, price, volume, and participant identifier — for a minimum of seven (7) years;
    - implement appropriate pre-trade and post-trade controls; and
    - maintain documented procedures for platform outages including client notification and order management during downtime.
24. Trading platform operators must report suspected market manipulation detected through their surveillance systems to the FSC promptly, without waiting for the conclusion of any internal investigation.

7.14 Virtual Asset Custodians

25. VASPs providing virtual asset custody services must, in addition to the general standards:
    - maintain robust key management procedures including appropriate use of hot and cold storage, multi-signature arrangements, and secure key generation and storage protocols;
    - ensure client virtual assets are stored securely, legally separate from the custodian's assets, and inaccessible to unauthorised persons;
    - maintain a complete and reconciled record of all client assets under custody, producible to the FSC on request;

- conduct regular independent audits of assets under custody and provide clients with periodic statements of their holdings;
- maintain a documented custody transfer or wind-down plan specifying how client assets would be returned or transferred in the event of the custodian ceasing operations; and
- disclose to clients all risks associated with the custody arrangements, including technical risks and treatment of assets in the event of insolvency.

8. Enforcement

26. Compliance with this Supervisory Rule is mandatory for all VASPs licensed under the Act. The FSC will monitor compliance through offsite monitoring, thematic reviews, and onsite inspections. Where a VASP fails to comply, the Commission may: issue a warning notice or formal direction to remediate; impose conditions on or vary the licence; suspend or revoke the licence; impose financial penalties; or publicly disclose enforcement actions taken. The Commission will take into account the nature, seriousness, and duration of the breach; whether it was deliberate or negligent; the VASP's compliance history; and remediation steps taken when determining the appropriate response.

9. Effective Date

27. The Commission will specify by notice. Adequate notice will be provided to licensees prior to the effective date.