



BERMUDA MONETARY AUTHORITY

DIGITAL ASSET BUSINESS ACT 2018

CODE OF PRACTICE

SEPTEMBER 2018

Contents

- I. INTRODUCTION 4
- II. PROPORTIONALITY PRINCIPLE..... 4
- III. CORPORATE GOVERNANCE 5
 - The Board..... 5
 - Oversight Responsibilities of the Board 6
 - Responsibility of the Chief and Senior Executives..... 7
- VI. SENIOR REPRESENTATIVE..... 7
- V. RISK MANAGEMENT FRAMEWORK..... 8
 - Risk Management Function 8
- VI. CLIENT DUE DILIGENCE AND MONITORING 9
- VII. INTEGRITY AND ETHICS 10
- VIII. DISCLOSURE OF INFORMATION 10
- IX. INTERNAL MANAGEMENT CONTROLS 0
 - Segregation and Protection of Client Assets..... 11
 - Competent and Effective Management..... 11
 - Delegation..... 11
 - Accounting and other Record Keeping..... 11
 - Adequate Personnel 12
 - Cybersecurity Programme 11
 - Internal Audit Function..... 13
 - Compliance Function..... 14
 - Self-Assessment..... 14
 - Fees 15
 - Client Agreements 15
 - Responsibility to Clients and Client Complaint Procedures 15
 - Conflicts of Interest..... 15
- X. OUTSOURCING..... 16
- XI. COOPERATION WITH REGULATORY AUTHORITIES..... 17

I. INTRODUCTION

1. This Code of Practice (the Code) is made pursuant to section 6 of the Digital Asset Business Act 2018 (the Act). Section 6 requires the Bermuda Monetary Authority (the Authority) to publish in such manner as it thinks fit, a Code that provides guidance on the duties, requirements, procedures, standards and sound principles to be observed by persons carrying on Digital Asset Business (DAB). Failure to comply with provisions set out in the Code will be a factor taken into account by the Authority in determining whether a licensed DAB is meeting its obligation to conduct its business in a sound and prudent manner.
2. The Code should be read in conjunction with the DAB Statement of Principles issued under section 5 of the Act.

II. PROPORTIONALITY PRINCIPLE

3. The Authority appreciates that DABs have varying risk profiles arising from the nature, scale, and complexity of the business, and that those DABs with higher risk profiles would require more comprehensive governance and risk management frameworks to conduct business in a sound and prudent manner.
4. Accordingly, the Authority will assess the DAB's compliance with the Code in a proportionate manner relative to its nature, scale, and complexity. These elements will be considered collectively, rather than individually (e.g. a DAB could be relatively small in scale, but carry out extremely complex business and therefore would still be required to maintain a sophisticated risk management framework). In defining these elements:
 - (a) Nature includes the relationship between clients and the DAB or characteristics of the service provided (e.g. a DAB that takes custody of a clients' assets versus one that does not, etc.);
 - (b) Scale includes size aspects such as volume of the business conducted or the size of the balance sheet in conjunction with materiality considerations (e.g. an assessment of the impact of a DAB's failure); and
 - (c) Complexity includes items such as organisational structures and product design.
5. In assessing the existence of sound and prudent business conduct, the Authority will have regard for both its prudential objectives and the appropriateness of each Code provision for the DAB, taking into account that DAB's nature, scale, and complexity.
6. The proportionality principle, discussed above, is applicable to all sections of the Code regardless of whether the principle is explicitly mentioned.

III. CORPORATE GOVERNANCE

7. The DAB must establish and maintain a sound corporate governance framework, which provides for appropriate oversight of the DAB's business and adequately recognises and protects the interests of clients. The framework should have regard for international best practice on effective corporate governance. Corporate governance includes principles of corporate discipline, accountability, responsibility, compliance, and oversight.
8. The ultimate responsibility for sound and prudent governance and oversight of the DAB rests with its board of directors or equivalent governing body (the board). In this regard, the board is responsible for ensuring corporate governance policies and practices are developed and applied in a prudent manner that promotes the efficient, objective and independent judgment and decision making by the board. The board must also have adequate powers and resources to be able to discharge its duties fully and effectively.

The Board

9. The Authority recognises that the board plays a critical role in the successful operation of a DAB. The board is chiefly responsible for setting corporate strategy, reviewing and monitoring managerial performance and determining an acceptable level of risk. Therefore, the effectiveness of the DAB's board is a basic tenet of the Authority's risk-based supervisory approach. Pragmatically, the board will likely delegate tasks; however, the delegation of authority to board committees, chief and senior executives, employees, or external parties does not absolve the board from its ultimate responsibilities.
10. The board must ensure that the business is effectively directed and managed, and conducted in a professional manner with appropriate integrity, and due care. It is the responsibility of the board to ensure that processes exist to assess and document the fitness and propriety of its members, controllers, and officers. The board must also take into account the fact that conflicts, or potential conflicts of interest, may on occasion preclude the involvement of specific individual members on particular issues or decisions.
11. To effectively discharge its duties, the board must have an appropriate number and mix of directors to ensure that it has requisite experience, knowledge, skills and expertise commensurate with the nature, scale and complexity of the DAB's business.
12. Individual board members must:
 - (a) act in good faith, honestly and reasonably exercise due care and diligence;
 - (b) ensure the interests of clients are protected;
 - (c) exercise independent judgment and objectivity in his/her decision making;and

- (d) ensure appropriate policies and procedures exist to effectively deal with conflicts of interest.

Oversight Responsibilities of the Board

13. As the DAB's governing body, a key responsibility is setting appropriate strategies and overseeing the implementation. This includes ensuring that chief and senior executives establish a framework to implement the DAB's strategic business objectives.
14. The board is also responsible for providing suitable oversight of the DAB's governance, risk management and internal controls frameworks, including any activities and roles that are delegated or outsourced. A list of oversight responsibilities that the board must consider when establishing and assessing the effectiveness of the corporate governance framework include ensuring the existence of:
- An operational framework (including risk management, internal audit and compliance functions) to ensure adequate oversight responsibilities so that sound corporate governance exists throughout the organisation;
 - Processes to assess and document the fitness and propriety of board members, controllers, the chief and senior executives, senior representative, and third-party service providers, including auditors, custodians, investment managers, etc.;
 - Board committees (where required) to provide oversight of both key operational areas, including finance and investments;
 - Policies and procedures to ensure adequate board oversight of the chief and senior executives;
 - Processes for the engagement and dismissal of the chief and senior executives and third-party service providers;
 - Policies and procedures to manage and mitigate conflicts of interest;
 - Processes to ensure key employees are adequately skilled to execute and discharge their duty and are compensated in a manner that encourages sound risk management and compliance;
 - Clearly defined charters, roles and responsibilities for the board, committees, chief and senior executives, and other key employees;
 - Business and operational strategies, plans, budgets, and significant policies and procedures including those surrounding oversight;
 - Review and approval of significant policies and procedures promoting effective corporate governance across the organisation, including those for risk management and internal controls, internal audit, and compliance functions;
 - Clear documentation and regular review of processes regarding the roles and responsibilities of the board, the chief and senior executives, and other key employees delegated corporate governance responsibilities (including appropriate segregation of the oversight function from management responsibilities);
 - Adequate independence for the risk management, internal audit, and

compliance functions to assist in oversight responsibilities and ensure these functions have a direct communication channel to the board and relevant committees; and

- Processes to confirm that the board has appropriate access to accurate, relevant, and timely information to enable it to carry out its duties and functions, including the monitoring and review of the performance and risk exposures of the DAB and the performance of the chief and senior executives.

Responsibility of the Chief and Senior Executives

15. The board must ensure that great care is taken in the selection of the chief and senior executives given the important role these play. In addition to supporting the board, the chief and senior executives are also responsible for the prudent administration of the DAB. Such responsibilities include:

- Manage and execute the day-to-day operations of the DAB, subject to the mandate established by the board and the laws and regulations in the operating jurisdiction;
- Assist the board to develop and implement an appropriate control environment including those around reporting and security systems;
- Provide recommendations on strategic plans, objectives, key policies, and procedures to the board for evaluation and authorisation;
- Assist the board with its oversight responsibilities by ensuring that the board has accurate and timely information, allowing the board to conduct robust and candid discussions on operational performance, strategy, and major policies, and to appraise the performance of management;
- Support oversight of both internal control functions (e.g. risk management, internal audit, compliance) and external third-party services;
- Ensure that key functions assigned corporate governance responsibilities are supported with adequate resources to execute and discharge their duties; and
- Ensure that external service providers, including approved auditors, have adequate resources and information to fulfil their role, including access to timely and accurate internal and outsourced records.
- Ensure the proper vetting of all staff.

Given the governance responsibilities, where requirements are imposed upon the DAB throughout the Code, the Authority will look to, and expect, the chief and senior executives, and ultimately the board, to ensure compliance.

VI. SENIOR REPRESENTATIVE

16. The role of the approved senior representative is integral to the BMA's DAB supervisory and regulatory framework. While the DAB's board and the chief and senior executives have primary responsibility for the conduct and performance of the DAB, the approved senior representative acts in an "early warning" role and monitors the DAB's compliance

with the Act on a continuous basis in accordance with Section 20 of the Act.

17. The Act requires every DAB to appoint a senior representative who must be resident in Bermuda, and to maintain a head office in Bermuda. The appointed senior representative must be knowledgeable in digital asset business and related Bermuda laws and regulations.
18. The approved senior representative would generally be a director or senior executive of the DAB who, under Section 20 of the Act, has the legislated duty to report certain events to the Authority.
19. The board and chief and senior executives must make arrangements to enable the approved senior representative to undertake his/her duties pursuant to the Act in an efficient and effective basis, including providing access to relevant records.

V. RISK MANAGEMENT FRAMEWORK

20. The board and the chief and senior executives should, based on their judgement, adopt an effective risk management and internal controls framework. The framework should have regard for international best practice on risk management and internal controls. This includes ensuring the fitness and propriety of individuals responsible for the management and oversight of the framework.

Risk Management Function

21. The DAB must establish a function to assist it with the oversight responsibility of the organisation's risk management framework. Depending on its risk profile, the function may be headed by a Chief Risk Officer or the responsibilities assigned to, or shared amongst, the DAB's operational unit leaders. Regardless, there should be a mechanism to allow direct reporting to the board or its established committees.
22. The risk management function should include:
 - Clearly defined and documented roles and responsibilities that are reviewed and approved by the board on a frequent basis;
 - A sound and effective risk management framework including developing (with the support of operational unit leaders) policies, procedures, and internal controls promoting the identification, assessment, monitoring, and reporting of material risks in a timely manner;
 - Establishing key policies (e.g. risk policy, cybersecurity policy, customer private key storage policy, and policies required under the Proceeds of Crime Anti Money Laundering, etc.) and assessing effectiveness and compliance with established benchmarks such as risk appetite and risk tolerance limits;
 - Employing measurement techniques such as benchmarking or stress and scenario testing; and
 - Reviewing on a regular basis the risk management techniques employed in

light of changing operational, regulatory, and market developments to ensure continued effectiveness and adoption of the international best practice.

- Operation policies for the transfer of assets between wallets which requires additional signatures from senior management based on the amount being transferred.

23. Risk management, risk identification, risk assessment, risk monitoring and risk reporting are critical for an effective risk management framework. As such, the DAB must implement these in an effective manner for the benefit of the DAB's stakeholders and to support its business objectives.

VI. CLIENT DUE DILIGENCE AND MONITORING

24. Industry participants, including clients, have the potential to adversely impact a jurisdiction's reputation and bring harm to society at large. Accordingly, the DAB must have procedures in place to ensure that proper due diligence is carried out before a decision is made to act for any new client. At a minimum, the DAB needs to be able to comply with The Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing Supervision and Enforcement) Act 2008, the Proceeds of Crime (Anti-Money Laundering and Anti-Terrorist Financing) Regulations 2008 and the Anti-Terrorism (Financial and Other Measures) Act 2004, together with any other relevant legislation that may come into force from time to time.

25. The duty of vigilance includes verification, recognition and reporting of suspicious transactions, the keeping of "know your client records", and delivering the appropriate Anti-Money Laundering training to all staff. The DAB must ensure that its procedures enable it to determine and verify the true identity of customers requesting its services. Copies of photo identification such as a driver's licence or passport should be retained in compliance with the Proceeds of Crime Act 1997 and relevant guidance notes and codes. The DAB must undertake due diligence checks on clients to protect against illegal activity, including money laundering and terrorist financing.

26. Where appropriate, measures that the DAB should consider putting in place to minimise the risk of abuse, include (depending upon client risk ratings) appropriate standard rules relating to maximum individual transaction sizes for its different digital asset services. In such cases, the DAB should have the ability to collate and aggregate individual transactions that may form part of a larger transaction and may be intended to avoid standard limits or reporting requirements.

27. The DAB must maintain detailed records for both sides of a transaction that includes: information to identify the parties, the public key addresses or accounts involved, the nature and date of the transaction, and the amount transferred. The DAB must monitor transactions for the purpose of detecting those which lack originator and/or beneficiary information, and take appropriate measures. These measures may include taking action

to freeze an account or to prohibit conducting transactions with designated persons and entities.

28. As part of protecting its clients and the jurisdiction's reputation, the DAB should have policies related to market manipulation and the appropriate use of its products and services. Where the DAB suspects or detects that abuse; such as spoofing or washing trading has taken place, the DAB should report such to the Authority and take the appropriate action including account closure and termination of the business relationship with the offending party.

VII. INTEGRITY AND ETHICS

29. The DAB must conduct its business with integrity at all times, acting with due care, skill and diligence. It must deal fairly with all clients and seek to ensure that clients are not misled as to the service being provided and the duties and obligations of the DAB.

VIII. DISCLOSURE OF INFORMATION

30. Any obligation to observe the confidentiality of information communicated by clients must be adhered to by the DAB (including its shareholders, directors, officers, senior executives, employees, outsourced partners, etc.) - unless the DAB is given relevant consent, is required by applicable law to disclose information, or provides information in accordance with the terms of the client constitutional documents. Accordingly, persons who have access to the DAB's confidential information should be advised in writing upon engagement. Further, the DAB should provide periodic reminders thereafter of confidentiality issues.
31. To comply with its duty to uphold integrity and ethics, the DAB's communication with clients and prospective clients must be clear and a fair representation. This includes marketing and promotional material. The DAB's public platform or materials provided to prospective clients prior to entering into an arrangement must include details of the board, the chief and senior executive team, head office (and registered office, if different), description of the complaints procedure, and arrangements in case of business failure. The DAB must disclose to clients any material business changes that impact clients.
32. For transparency purposes, the DAB must also ensure that its status as a licensed undertaking is disclosed in all advertisements and correspondence. The following wording is suggested:

“Company X is licensed to conduct digital asset business by the Bermuda Monetary Authority.”

IX. INTERNAL MANAGEMENT CONTROLS

33. The board and the chief and senior executives must review and assess the effectiveness of the internal reporting and operating controls. Any material deficiencies must be documented and resolution measures should be implemented in a timely manner. The board and the chief and senior executives should ensure the implementation of policies and procedures requiring that internal control weaknesses are reported directly to the board and chief and senior executives.

Segregation and Protection of Client Assets

34. Section 18 (1) of the Act directs a DAB to ensure that any assets belonging to clients are kept segregated from the DAB's own assets. The DAB may place client assets in a trust with a qualified custodian, or have a surety bond or indemnity insurance, or implement other arrangements to ensure the return of client assets in the event the DAB is placed into liquidation, becomes insolvent or is a victim of theft. While keeping separate from its own, the DAB may commingle client assets where such would benefit clients; however, proper accounting must be in place to accurately allocate each holding to the respective client.
35. The DAB must have mechanisms in place to assess its liquidity needs, including sums required for trading and other client transaction types. These mechanisms must be used to inform the DAB's client private key storage policy. The client private key storage policy should require that the majority of client private keys, not required for client transactions, should be held in cold storage to mitigate against client loss arising from cyber-attacks. The Authority also expects that only a minimal balance should be kept in hot storage and that the mechanism and thresholds for transfer between hot, cold and other storages should be well documented and audited.

Competent and Effective Management

36. The DAB should have competent management commensurate with the nature, scale and complexity of its business. The DAB must also have appropriate management resources to control the affairs of the licensed business, including ensuring compliance with legal obligations and standards under the Code.

Delegation

37. The board may delegate the administration and other duties to directors, chief and senior executives, employees or committees as it deems appropriate. When doing so, decisions should align with authorisation and signing powers outlined in policies and procedures, and regard must also be given to risks to stakeholder protection and applicable laws.

Accounting and other Record Keeping

38. Appropriate records must be kept and preserved in Bermuda. These records will at least include information for the DAB to effectively carry out its functions and comply with applicable law. Systems must be in place to ensure that decision-makers, regulators, clients and other relevant stakeholders can receive requisite information in a timely manner. This should include the identity of shareholders, directors, officers or business partners. In addition, records of account and client transactions must be maintained in accordance with the laws applicable to it.
39. The DAB's accounting and record keeping systems must support its compliance with regulatory reporting, such as the annual statutory and other returns, or other reporting that the Authority may require on an ad hoc basis in fulfilment of the Authority's regulatory oversight responsibilities.

Adequate Personnel

40. The DAB must have available suitable numbers of staff who are appropriately trained and competent to discharge their duties effectively. The DAB should ensure that the responsibilities and authority of each staff member are clear and appropriate given his/her qualifications and experience, and that staff receive the necessary training appropriate for their roles.
41. The DAB should ensure that it has in place systems, controls, policies and procedures, to ensure that staff members perform their duties in a diligent and proper manner. It is important that staff understand and comply with the established systems, policies and procedures including those dealing with new business acceptance, financial transactions, and staff training.

Cybersecurity Programme

42. In many respects, DAB is susceptible to risks such as cyber threats or systems failure. Accordingly, the DAB must have a comprehensive cybersecurity programme that is commensurate with the nature, scale and complexity of its business. Such should include a documented cybersecurity policy.
43. The DAB must implement a written cybersecurity policy setting forth the DAB's policies and procedures for the protection of its electronic systems, and client and counterparty data stored on those systems. The policies must be reviewed and approved by the DAB's board at least annually.
44. The cybersecurity policy must minimally address the following areas:
 - (a) information security;
 - (b) data governance and classification;
 - (c) access controls;
 - (d) business continuity and disaster recovery planning and resources;

- (e) capacity and performance planning;
 - (f) systems operations and availability concerns;
 - (g) systems and network security;
 - (h) systems and application development and quality assurance;
 - (i) physical security and environmental controls;
 - (j) customer data privacy;
 - (k) vendor and third-party service provider management;
 - (l) monitoring and implementing changes to core protocols not directly controlled by the DAB, as applicable; and
 - (m) incident response.
45. Further, the DAB must designate a qualified employee to serve as its Chief Information Security Officer (CISO) responsible for overseeing and implementing the DAB's cybersecurity programme and enforcing its cybersecurity policy.
46. The DAB must employ adequate cybersecurity personnel to manage its cybersecurity risks and provide opportunity and resources for cybersecurity personnel to stay abreast of changing cybersecurity threats and countermeasures. DAB's must require personnel to remain current.
47. An effective cybersecurity programme should be able to ensure the availability and functionality of the DAB's electronic systems, and to protect both those systems and any sensitive data stored on those systems (including customer assets) from unauthorised access, use, or tampering. The programme will also need to address risks arising from third-party vendors where there is system connectivity, and include policies related to hot and cold client private key storage.
48. Further, the cybersecurity programme should outline policies surrounding how the DAB will tackle market abuse and, where applicable, under what conditions it will halt trading, suspend or close offending client accounts and notify relevant authorities.
49. In summary, at a minimum, the DAB's cybersecurity programme will be required to satisfy five core functions:
- (a) identify internal and external risks;
 - (b) protect licensee electronic systems and the information stored on those systems;
 - (c) detect system intrusions, and breaches;
 - (d) respond to a detected event and mitigate negative effects; and
 - (e) recover from operational disruption to the normal course of business.
50. The DAB must annually commission an external independent audit of its cybersecurity programme. The external auditor's report must detail the review of the DAB's business processes, systems, policies and dependencies/relationships with the systems of third party partners and affiliates to confirm that control measures are adequate to ensure consistent compliance with the Act, related Rules and this Code.

51. The DAB must also be proactive in alerting the Authority to any significant developments relevant to its staffing or to its systems and controls environment. This includes any failure or breach of its systems that involve the loss of, the unlawful destruction of, or unauthorised access to, any personal identifiable information that it holds on its clients or any assets that it holds on behalf of its clients.

Internal Audit Function

52. Sound practice requires the implementation of the “Three Lines of Defence” with the first line being risk taking, and the second being risk-control and compliance. The third critical line is the internal audit. The DAB must have an internal audit function. The internal audit function should:

- Be segregated and staffed by persons adequately independent of operational functions, including risk management, compliance, operations and finance;
- Have clearly defined and documented charters, roles and responsibilities that are reviewed and approved by the board on a regular basis and that demonstrate the independence and separation of the function;
- Document material policies and procedures to be reviewed and approved by the board;
- Prepare an internal audit plan to ensure assessment of governance and controls of key risk areas at appropriate interval taking into consideration the nature, scale and complexity of the DAB (the internal audit plan should be reviewed at least annually and approved by the board of directors);
- Have unrestricted access to all areas of the organisation, including access to any records held by third-party service providers;
- Examine operational practices to ensure the adequacy and effectiveness of governance, risk management, policies, procedures, and controls;
- Report governance and control deficiencies directly to the board of directors or a committee appointed by the board;
- Establish a robust mechanism to monitor deficiencies until remediation efforts are completed and report remedial progress to the board at regular intervals taking into consideration the level of risk involved;
- Have appropriate authority within the organisation to ensure management addresses any internal audit findings and recommendations with respect to the adequacy and effectiveness of governance, risk management, policies, procedures and controls;
- Have sufficient resources and fit and proper staff to carry out duties and responsibilities;
- Have sufficient knowledge and experience to employ methodologies designed to assist the DAB in identifying key risks; and
- Assist the board to identify areas for improvement.

Compliance Function

53. Regulatory and other requirements (such as internal policies and procedures) are imposed for the protection of the DAB itself, clients and stakeholders more widely. The establishment of a function focused on how well the DAB adheres to the varied requirements is valuable. The DAB must develop a function to assist it to monitor and evaluate its compliance with jurisdictional laws and regulations, internal controls, policies, and procedures. The compliance function should also promote and sustain a corporate culture of compliance and integrity.

54. The compliance function should include:

- Policies, procedures and processes documenting the compliance with the risk management framework, legal and ethical conduct, applicable laws, rules and standards;
- System of compliance monitoring and testing, including a plan to address any deficiencies or non-compliance that may be identified;
- Training programs for staff on compliance issues, and provide a mechanism for staff to report confidentially concerns regarding compliance deficiencies and breaches.

Self-Assessment

55. The DAB must have a comprehensive and integrated forward-looking view of all material reasonably foreseeable risks that arise from its business model and interaction with the wider environment. This allows a more informed assessment of the appropriateness of its business strategy and enhances its ability to position itself for future success and sustainability. The DAB must, therefore, develop policies, processes, and procedures to assess all its material reasonably foreseeable risks over its forward-looking planning horizon and self-determine its capital (both quality and quantity), liquidity, and resourcing needs to inform its business strategy. The risk self-assessment must be performed at least annually and reported to the Authority. The DAB should be guided by the proportionality principle in establishing the risk self-assessment framework. Minimally, the assessment should:

- Be an integral part of the DAB's risk management framework;
- Be clearly documented, reviewed, and evaluated regularly by the board and the chief and senior executives to ensure continual advancement in light of changes in the strategic direction and market developments;
- Cover both all material reasonably foreseeable risks and a forward looking time horizon deemed appropriate by the board, having regard for the dynamics of the digital asset business industry and wider relevant influences;
- Ensure an appropriate oversight process whereby material deficiencies are reported on a timely basis and suitable actions are taken.

56. The DAB must ensure the fitness and propriety of key individuals overseeing and performing the assessment; this includes third-party service providers, if applicable, assisting with the assessment process.

Fees

57. The DAB is expected to exhibit proper transparency in its dealings with clients and potential clients and to act ethically and with integrity at all times. Terms of business, including fees and commissions for its different services must be explicitly disclosed prior to transactions, and any changes promptly brought to the attention of customers to ensure that there is no misunderstanding with regard to transaction charges and other fees.

Client Agreements

58. To ensure clients are dealt with fairly and are informed, the DAB must disclose terms of business with each prospective client, and keep a record of the terms of the agreement with each client, including evidence of the client's agreement to those terms. That agreement should include, but not be limited to, the following provisions:

- (a) a clear description of the services to be provided, fees to be charged and the manner in which fees are expected to be paid;
- (b) a general description of how, and by whom, requests for action are to be given;
- (c) a general description of any provisions for the termination of the agreement and the consequences of termination; and
- (d) a statement that the DAB is licensed by the Authority including the type of licence issued.

Responsibility to Clients and Client Complaint Procedures

59. The DAB must ensure that its business is conducted in such a way as to treat its clients fairly, both before the inception of the contractual arrangement and through to the point at which all obligations under a contract have been satisfied. The DAB must establish and implement policies and procedures to ensure that this occurs.
60. The DAB must ensure that the client complaints are properly logged and dealt with in a timely basis. A record of the details of the complaint, the DAB's response and any action taken as a result should be maintained.

Conflicts of Interest

61. Conflicts naturally arise in the course of business and may be exploited on account of information asymmetry. The DAB must ensure it has policies and procedures to mitigate conflicts to avoid harm to clients and stakeholders more widely, including policies and procedures regarding disclosing relevant information. The DAB need to implement

internal rules and procedures for dealing with conflicts of interest. Where conflicts cannot be avoided, the DAB must seek to ensure that the interests of clients are not damaged through undisclosed conflicts of interest.

62. This includes whether the conflict arises directly in the course of its own role or, as relevant, between the DAB and its service providers or, for example, between different classes of clients.
63. The nature and relative market cap of the digital asset business industry inherently exposes it to arbitrage and market valuation manipulation. With information asymmetry and global connectivity, the DAB's board, officers or staff may at times be positioned to exploit opportunities at the expense of stakeholders. The conflict of interest policies and procedures must also include measures that would prevent market manipulation such as insider trading, pump and dump or other schemes that may bring harm to clients.

X. OUTSOURCING

64. While the DAB may outsource certain important business roles (such as asset management, custodial services, cybersecurity, compliance, and internal audit) to third parties or affiliates, such action does not remove the responsibility from the DAB to ensure that all the requirements of the Act and related legislation, and this Code, are complied with to the same level as if these roles were performed in-house.
65. Where the DAB outsources roles either externally to third parties or internally to other affiliated entities, the board must ensure that there is oversight and clear accountability for all outsourced roles as if these functions were performed internally and subject to the DAB's own standards on governance and internal controls. The board should also ensure that the service the agreement includes terms on compliance with jurisdictional laws and regulations. Agreements should not prohibit cooperation with the Authority, and the Authority's access to data and records in a timely manner.
66. Where the board has outsourced a role and/or is considering outsourcing a role, the board must assess the impact or potential impact on the DAB. The board must not outsource a role that is reasonably expected to adversely affect the DAB's ability to operate in a prudent manner. These considerations include where outsourcing is reasonably expected to:
 - Adversely affect the DAB's governance and risk management structures;
 - Unduly increase operational risk;
 - Affect the Authority's ability to effectively supervise and regulate the DAB; and
 - Adversely affect client protection.

XI. COOPERATION WITH REGULATORY AUTHORITIES

67. The DAB is expected to deal openly and in a spirit of cooperation with the Authority and any other relevant regulatory authorities. This includes ensuring that any outsourced vendors are aware of their role in assisting the DAB in meeting its obligations under the Act and related legislation, and this Code.
68. The DAB should also ensure that any contracts or agreements that it enters into does not intentionally, or otherwise, frustrate the Authority's ability to carry out its supervisory or regulatory obligations in relation to the DAB.
