# AIFC RULES ON DIGITAL ASSET ACTIVITIES (DAA)
# AIFC RULES NO. FR00062 OF 2023
**(with amendments as of 13 April 2025, which commence on 13 October 2025)**

**Approval date: 10 September 2023**

**Commencement date: 01 January 2024**

## CONTENTS

# 1. GENERAL

## 1.1. Application of these Rules

(1) These Rules, which may be cited as the AIFC Rules on Digital Asset Activities ("DAA"), apply to a Person carrying out, in or from the AIFC, the following Regulated Activities in relation to Digital Assets:

(a) Dealing in Investments as Principal;

(b) Dealing in Investments as Agent;

(c) Managing Investments;

(d) Managing a Collective Investment Scheme;

(e) Providing Custody;

(f) Arranging Custody;

(g) Advising on Investments;

(h) Arranging Deals in Investments;

(i) Providing Money Services; and

(j) Operating a Digital Asset Trading Facility.

(2) Except as stated otherwise, a reference to Digital Asset in these Rules it taken to include Digital Asset Derivatives.

**Guidance:**

The following activities do not constitute Operating a Digital Asset Business:

(a) trading of Digital Assets for the Person's own investment purposes, where such trading is not carried out by way of business; or

(b) any other activity or arrangement that is deemed by the AFSA to not constitute Operating a Digital Asset business, where necessary and appropriate in order for the AFSA to pursue its objectives.

## 2. RULES APPLICABLE TO DIGITAL ASSET TRADING FACILITY OPERATORS

This Chapter 2 applies to all Digital Asset Trading Facility Operators.

**Guidance**

A Digital Asset Trading Facility Operator is an Authorised Firm to which provisions of the Constitutional Statute, FSFR, GEN, COB, AML, and MAR are applicable either directly or in respect of its officers and Employees who are Approved Individuals or Designated Individuals:
Article 4-1 of the Constitutional Statute;
FSFR (in whole);
AML (in whole);
Chapter 2 (Client classification) of the COB;
Chapter 3 (Communications with Clients and Financial Promotions) of the COB;
Chapter 4 (Key information and client agreement) of the COB;
Chapter 7 (Conflicts of interest) of the COB;
Chapter 8 (Client Assets) of the COB;
Chapter 9 (Reporting to Clients) of the COB;
Chapter 15 (Complaints handling and dispute resolution) of the COB;
Chapter 5 (Market Abuse) of the MAR;
Chapter 2 (Controlled and Designated Functions) of the GEN;
Chapter 3 (Control of Authorised Persons) of the GEN;
Chapter 4 (Core Principles) of the GEN;
Chapter 5 (Systems and Controls) of the GEN;
Chapter 6 (Supervision) of the GEN; and
Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC.

### 2.1. Authorisation

(1) A Person wishing to carry out the Regulated Activity of Operating a Digital Asset Trading Facility must be an Authorised Firm licensed by the AFSA.

(2) A Person wishing to carry out the Regulated Activity of Operating a Digital Asset Trading Facility must submit to the AFSA relevant policies and controls.

### 2.2. Requirements for Digital Asset Trading Facility Operator authorisation

The AFSA may not grant authorisation or variation to operate a Digital Asset Trading Facility unless the applicant satisfies all of the following requirements:

(1) general authorisation requirements applicable to the applicant under the Framework Regulations and other applicable rules, and

(2) the applicant must ensure that it maintains at all times capital resources in the amount specified in Table 1 by reference to the activity that the Authorised Firm is licensed to conduct or, if it is authorised to conduct more than one such activity, the amount that is the higher or highest of the relevant amounts in Table 1.

**Table 1**

| Regulated Activity | Capital requirement (USD) |
|---|---|
| Operating a Digital Asset Trading Facility | The higher of (i) 200,000 or (ii) an amount equal to sufficient working capital in fiat currency to continue business for a period of 12 months, based on realistic forecasts for the |

| | |
|---|---|
| | business in different market conditions (both negative and positive scenarios) |
| Providing Custody (in relation to Digital Assets) | 250,000 |

(3) In determining whether the Digital Asset Trading Facility Operator meets the capital requirement(s) and, in particular, has sufficient working capital to continue business on a go-forwards basis, the Digital Asset Trading Facility Operator must have regard to the following matters:

(a) the business carried out, or to be carried out by the Digital Asset Trading Facility Operator;

(b) the risks to the continuity of the services provided by, or to be provided by, the Digital Asset Trading Facility Operator, including any outsourced services (including services outsourced to a Group entity where applicable);

(c) the liabilities to which the Digital Asset Trading Facility Operator is exposed or could be exposed to, including as a result of any failure by any third party; and

(d) the means by which the Digital Asset Trading Facility Operator manages and, if the Digital Asset Trading Facility Operator is a member of a Group, by which other members of the Group manage, the occurrence of risk in connection with the Digital Asset Trading Facility Operator's business.

**Guidance**

Intangible assets, including goodwill, cannot be used as part of determining whether the capital requirement value is met or whether the Digital Asset Trading Facility Operator has sufficient working capital, and must be disregarded when determining whether the requirements are met for the purposes of Table 1.

## 2.3. Governance

### 2.3.1. Mandatory appointments

(1) A Digital Asset Trading Facility Operator must make the following appointments:

(a) Senior Executive Officer;

(b) Finance Officer;

(c) Compliance Officer; and

(d) Money Laundering Reporting Officer.

(2) A Digital Asset Trading Facility Operator must appoint a Chief Information Technology Officer, who is an individual responsible for its ongoing information technology ("IT") operations, maintenance and security oversight, and for ensuring that the Digital Asset Trading Facility Operator's IT systems are reliable and adequately protected from external attack or incident.

(3) AFSA may direct a Digital Asset Trading Facility Operator to appoint a Risk Manager.

(4) A person may not combine two roles specified in (1) unless the Digital Asset Trading Facility Operator obtains the AFSA's written approval.

### 2.3.2. Board of Directors of a Digital Asset Trading Facility Operator

(1) A Digital Asset Trading Facility Operator must have an effective Board of Directors which is collectively accountable for ensuring that the Digital Asset Trading Facility Operator's business is managed prudently and soundly. At least one-third of the Board of Directors should comprise independent Directors.

*Note: Rule 2.3.2(1) will come into force 12 months after the commencement of these Rules.*

(2) The AFSA may issue guidance on the requirements relating to Board composition, structure, duties and powers as well as skills, experience and qualifications of Directors, and other relevant requirements.

(3) The Board must ensure that there is a clear division between its responsibility for setting the strategic aims and undertaking the oversight of the Digital Asset Trading Facility Operator and the senior management's responsibility for managing the Digital Asset Trading Facility Operator's business in accordance with the strategic aims and risk parameters set by the Board.

(4) The Board and its committees must have an appropriate balance of skills, experience, independence, and knowledge of the Digital Asset Trading Facility Operator's business, and adequate resources, including access to expertise as required and timely and comprehensive information relating to the affairs of the Digital Asset Trading Facility Operator.

(5) The Board must ensure that the Digital Asset Trading Facility Operator has an adequate, effective, well-defined and well-integrated risk management, internal control and compliance framework.

(6) The Board must ensure that the rights of shareholders are properly safeguarded through appropriate measures that enable the shareholders to exercise their rights effectively, promote effective dialogue with shareholders and other key stakeholders as appropriate, and prevent any abuse or oppression of minority shareholders.

(7) The Board must ensure that the Digital Asset Trading Facility Operator's financial and other reports present an accurate, balanced and understandable assessment of the Digital Asset Trading Facility Operator's financial position and prospects by ensuring that there are effective internal risk control and reporting requirements.

(8) A Director of the Digital Asset Trading Facility Operator must act:

(a) on a fully informed basis;

(b) in good faith;

(c) honestly;

(d) with due skill, care and diligence; and

(e) in the best interests of the Digital Asset Trading Facility Operator and its shareholders and Clients.

## 2.4. Technology resources

### 2.4.1. Sufficient resources

In addition to appropriate systems, resources and controls, a Digital Asset Trading Facility Operator must have sufficient technology resources to continually operate, maintain, and supervise its facility.

### 2.4.2. Confidentiality

A Digital Asset Trading Facility Operator must take reasonable steps to ensure that its information, records and data are secure, and the confidentiality is maintained.

### 2.4.3. Cyber-security

A Digital Asset Trading Facility Operator must take reasonable steps to ensure that its IT systems are reliable and adequately protected from external attack or incident, as well as from risks that can arise from inadequacies or failures in the Digital Asset Trading Facility Operator's processes and systems and, as appropriate, the systems of third-party suppliers, agents and others. This includes the fact that a Digital Asset Trading Facility Operator must ensure there are the necessary resources in place to manage these risks.

### 2.4.4. Cyber-security policy

(1) A Digital Asset Trading Facility Operator must implement a written cyber-security policy setting forth its policies and procedures for the protection of its electronic systems, Members and counterparty data stored on those systems, which must be reviewed and approved by the Digital Asset Trading Facility Operator's Board of Directors at least on an annual basis.

(2) The cyber-security policy must, as a minimum, 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) appropriateness of systems (including the allocation of responsibilities between internal IT functions and reliance on third party systems);

(g) systems operations and availability concerns;

(h) systems and network security;

(i) systems and application development and quality assurance;

(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and third-party service provider management;

(m) incident response; and

(n) arrangements and methods for periodically reviewing and evaluating the effectiveness of the systems.

(3) A Digital Asset Trading Facility Operator must inform the AFSA immediately if it becomes aware, or has reasonable grounds to believe, that a significant breach by any Person of its cyber-security policy may have occurred or may be about to occur.

(4) A Digital Asset Trading Facility Operator must consider the impact of any outsourcing arrangements, as well as the interoperability risks when dealing with systems and software provided by third parties.

(5) (A Digital Asset Trading Facility Operator must ensure all staff receive appropriate training in relation to cybersecurity.

### 2.4.5. On-going monitoring

For the purposes of meeting the requirement in DAA 2.4.1, a Digital Asset Trading Facility Operator must have adequate procedures and arrangements for the evaluation, selection and on-going maintenance and monitoring of IT systems. Such procedures and arrangements must, at a minimum, provide for:

(a) incident and problem management and system change;

(b) testing IT systems before live operations in accordance with the requirements in DAA 2.4.6. and 2.4.7;

(c) real time monitoring and reporting on system performance, availability and integrity; and

(d) adequate measures to ensure:

(i) the IT systems are resilient and not prone to failure;

(ii) (ii) business continuity in the event that an IT system fails;

(iii) (iii) protection of the IT systems from damage, tampering, misuse or unauthorised access; and

(iv) (iv) the integrity of data forming part of, or being processed through, IT systems.

### 2.4.6. Testing of technology systems

A Digital Asset Trading Facility Operator must, before commencing live operation of its IT systems or any updates thereto, use development and testing methodologies in line with internationally accepted testing standards in order to test the viability and effectiveness of such systems. For this purpose, the testing must be adequate for the Digital Asset Trading Facility Operator to obtain reasonable assurance that, as a minimum, the systems:

(a) enable it to comply with all the applicable requirements on an on-going basis;

(b) can continue to operate effectively in stressed market conditions;

(c) have sufficient electronic capacity to accommodate reasonably foreseeable volumes of messaging and orders;

(d) are adequately scalable in emergency conditions that might threaten the orderly and proper operations of its facility; and

(e) embed any risk management controls, such as generating automatic error reports, which work as intended.

### 2.4.7. Testing relating to Members' technology systems

(1) A Digital Asset Trading Facility Operator must implement standardised conformance testing procedures. A Digital Asset Trading Facility Operator must ensure that the systems which its Members are using to access facilities operated by it have a minimum level of functionality that is compatible with its IT systems and will not pose any threat to fair and orderly conduct of its facility.

(2) A Digital Asset Trading Facility Operator must also require its Members, before commencing live operation of any electronic trading system, user interface or a trading algorithm, including any updates to such arrangements, to use adequate development and testing methodologies to test the viability and effectiveness of their systems, to include system resilience and security.

(3) The requirements in (1) and (2) do not apply to the Member of a Digital Asset Trading Facility Operator if the Member is a Body Corporate or an individual (natural person) that carries out the activity solely as principal.

### 2.4.8. Regular review of systems and controls

(1) A Digital Asset Trading Facility Operator must undertake at least an annual review of its IT systems and controls as appropriate to the nature, scale and complexity of its operations, the diversity of its operations, the volume and size of transactions, and the level of risk inherent with its business.

(2) For the purposes of (1), a Digital Asset Trading Facility Operator must adopt well defined and clearly documented development and testing methodologies which are in line with internationally accepted testing standards.

(3) After the review is complete, a Digital Asset Trading Facility Operator must promptly remedy any deficiencies discovered during the review and keep a record of the review and its findings for a period of 6 years from the review. This record must be provided promptly to the AFSA on request.

### 2.4.9. Mandatory third-party audit of technology governance and IT systems

(1) A Digital Asset Trading Facility Operator is required to undergo a qualified independent third-party technology governance and IT audit to conduct vulnerability assessments and penetration testing at least on an annual basis.

(2) A Digital Asset Trading Facility Operator must provide the results of technology governance and IT assessments and tests to the AFSA on its request.

(3) The AFSA may publish a list of requirements that should be met by qualified auditors who conduct independent third-party technology governance and IT audit.

**Guidance:**

Credentials which indicate a qualified independent third-party auditor is suitable to conduct audit of technology governance and IT systems may include:

(1) designation as a Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association (ISACA); or

(2) designation as a Certified Information Systems Security Professional (CISSP) by the International Information System Security Certification Consortium (ISC); or

(3) accreditation by a recognised and reputable body to certify compliance with relevant ISO/IEC 27000 series standards; or

(4) accreditation by the relevant body to certify compliance with the Kazakhstani standards in the area of information (cyber) security.

### 2.4.10. Systems and controls

(1) A Digital Asset Trading Facility Operator must ensure that it has appropriate systems and controls to address the risks to its business. Such systems and controls should be developed considering such factors as the nature, scale and complexity of the Digital Asset Trading Facility Operator's business, the diversity of its operations, the volume and size of transactions, and the level of risk inherent with its business.

(2) A Digital Asset Trading Facility Operator must, as a minimum, have in place systems and controls with respect to the procedures describing the creation, management and control of Digital wallets and private keys, as well as the infrastructure to deal with updates and technological changes such as forks.

(3) A Digital Asset Trading Facility Operator must have adequate systems and controls to enable it to calculate and monitor its capital resources and its compliance with the requirements in DAA 2.2.(2). The systems and controls must be in writing and must be appropriate for the nature, scale and complexity of the Digital Asset Trading Facility Operator's business and its risk profile.

(4) A Digital Asset Trading Facility Operator must have due regard to its obligations to keen data secure, including the safe storage and transmission of data in accordance with clear protocols.

### 2.4.11. Technology governance

A Digital Asset Trading Facility Operator must, as a minimum, have in place systems and controls with respect to the following:

(a) Procedures describing the creation, management and controls of Digital wallets, including:

(i) wallet setup/configuration/deployment/deletion/backup and recovery;

(ii) wallet access management;

(iii) wallet user management;

(iv) wallet rules and limit determination, review and update; and

(v) wallet audit and oversight.

(b) Procedures describing the creation, management and controls of private and public keys, including, as applicable:

(i) private key generation;

(ii) private key exchange;

(iii) private key storage;

(iv) private key backup;

(v) private key destruction;

(vi) private key access management;

(vii) public key sharing; and

(viii) public key re-use.

(c) Systems and controls to mitigate the risk of misuse of Digital Assets and money laundering and terrorist financing risks, setting out how:

(i) the origin of Digital Assets is determined, in case of an incoming transaction; and

(ii) the destination of Digital Assets is determined, in case of an outgoing transaction.

(d) A security plan describing the security arrangements relating to:

(i) the privacy of sensitive data;

(ii) networks and systems;

(iii) cloud based services;

(iv) physical facilities; and

(v) documents, and document storage.

(e) A risk management plan containing a detailed analysis of likely risks with both high and low impact, as well as mitigation strategies. The risk management plan must cover, but is not limited to:

(i) operational risks;

(ii) technology risks, including 'hacking' related risks;

(iii) market risk for each Digital Asset; and

(iv) risk of Financial Crime.

## 2.5. Requirements applicable to a Digital Asset Trading Facility Operator

### 2.5.1. Business Rules, Membership Rules and Admission to Trading Rules

(1) A Digital Asset Trading Facility Operator must prepare Business Rules, Admission to Trading Rules, and Membership Rules (the "DATF Operator's Rules").

(2) A Digital Asset Trading Facility Operator must seek prior approval of any of the DATF Operator's Rules and of amendments to any of its Rules by obtaining approval of the AFSA.

(3) Members and Clients of a Digital Asset Trading Facility must be notified at least 10 days before approved by the AFSA amendments are introduced to the relevant rules of the DATF Operator.

### 2.5.2. Content of Business Rules

(1) A Digital Asset Trading Facility Operator's Business Rules must:

(a) be based on objective criteria;

(b) be non-discriminatory;

(c) be clear, fair and not misleading;

(d) set out the Members' and other participants' obligations:

(i) arising from the Digital Asset Trading Facility Operator's constitution and other administrative arrangements;

(ii) when undertaking transactions on its facility; and

(iii) relating to professional standards that must be imposed on staff and agents of the Members and other participants when undertaking transactions on its facility;

(e) be made publicly available free of charge;

(f) contain provisions for the resolution of Members' and other participants' disputes and an appeal process for the decisions of the Digital Asset Trading Facility Operator, whether by an independent internal body or otherwise; and

(g) contain disciplinary procedures, including any sanctions that may be imposed by the Digital Asset Trading Facility Operator against its Members and other participants.

(2) A Digital Asset Trading Facility Operator must incorporate into its Business Rules the substance of additional provisions relevant to Derivatives to be found in the AMI and COB Rules, for the purpose of regulating operations in Digital Assets Derivatives.

### 2.5.3. Monitoring and enforcing compliance with Business Rules

A Digital Asset Trading Facility Operator must have effective arrangements for monitoring and enforcing compliance with its Business Rules including procedures for:

(a) prompt investigation of complaints made to the Digital Asset Trading Facility Operator about the conduct of Persons in the course of using the Digital Asset Trading Facility Operator's facility; and

(b) where appropriate, disciplinary action resulting in financial and other types of penalties.

### 2.5.4. Financial penalties

If arrangements made pursuant to DAA 2.5.3. include provision for requiring the payment of financial penalties, they must include arrangements for ensuring that any amount so paid is applied only in one or more of the following ways:

(a) towards meeting expenses incurred by the Digital Asset Trading Facility Operator in the course of the investigation of the breach or course of conduct in respect of which the penalty is paid, or in the course of any appeal against the decision of the Digital Asset Trading Facility Operator in relation to that breach or course of conduct; or

(b) for the benefit of Members and Clients of the Digital Asset Trading Facility Operator's facility.

### 2.5.5. Appeals

Arrangements made pursuant to DAA 2.5.3. must include provision for fair, independent and impartial resolution of appeals against decisions of the Digital Asset Trading Facility Operator.

### 2.5.6. Membership Rules

The Membership Rules of a Digital Asset Trading Facility Operator must specify the obligations imposed on Members and Clients of its facility arising from:

(a) the constitution and administration of the facility;

(b) where appropriate rules relating to transactions using its facilities;

(c) admission criteria for Members, which must comply with DAA 2.6.2;

(d) where appropriate rules and procedures for clearing and settlement of transactions; and

(e) where appropriate rules and procedures for the prevention of Market Abuse, money laundering and Financial Crime.

### 2.5.7. Admission to Trading Rules

(1) A Digital Asset Trading Facility Operator must make clear and transparent rules concerning the admission of Digital Assets to trading on its facility.

(2) The Admission to Trading Rules of the Digital Asset Trading Facility Operator must ensure that Digital Assets admitted to trading on a facility of the Digital Asset Trading Facility Operator are:

(a) capable of being traded in a fair, orderly and efficient manner; and

(b) freely negotiable.

## 2.6. Membership

### 2.6.1. Persons eligible for Membership

A Digital Asset Trading Facility Operator may only admit as a Member a Person who satisfies the admission criteria set out in its Membership Rules and which is:

(a) an Authorised Firm whose Licence permits it to carry out the Regulated Activities of Dealing in Investments as Principal or Dealing in Investments as Agent;

(b) a Recognised Non-AIFC Member; or

(c) a Body Corporate or an individual (natural person) which carries out the activity solely for its own investment purposes, where such trading does not constitute Dealing in Investments as Principal by way of business.

### 2.6.2. Admission criteria

(1) A Digital Asset Trading Facility Operator must ensure that access to its facility is subject to criteria designed to protect the orderly functioning of the market and the interests of investors generally.

(2) A Digital Asset Trading Facility Operator may only give access to or admit to membership a Person who:

(a) is fit and proper and of good repute;

(b) if applicable, has a sufficient level of ability, competence and experience, including appropriate standards of conduct for its staff; and

(c) if applicable, has adequate organisational arrangements, including financial and technological resources.

(3) In assessing whether access to a Digital Asset Trading Facility Operator's facility is subject to criteria designed to protect the orderly functioning of the market and the interests of investors, the AFSA may have regard to whether:

(a) the Digital Asset Trading Facility Operator limits access as a Member to such Persons:

(i) over whom it can with reasonable certainty enforce its rules contractually;

(ii) who have sufficient technical competence to use its facilities; and

(iii) if appropriate, who have adequate financial resources in relation to their exposure to the Digital Asset Trading Facility Operator;

(b) indirect access to the Digital Asset Trading Facility Operator's facility is subject to suitable criteria, remains the responsibility of a Member of the Digital Asset Trading Facility Operator and is subject to the Digital Asset Trading Facility Operator's rules; and

(c) the Digital Asset Trading Facility Operator's rules:

(i) set out the design and operation of the Digital Asset Trading Facility Operator's relevant systems;

(ii) set out the risk for Members and Clients when accessing and using the Digital Asset Trading Facility Operator's facilities;

(iii) contain provisions for the resolution of Members' and Clients' disputes and an appeal process for the decisions of the Digital Asset Trading Facility Operator;

(iv) contain disciplinary proceedings, including any sanctions that may be imposed by the Digital Asset Trading Facility Operator against its Members and Clients; and

(v) set out other matters necessary for the proper functioning of the Digital Asset Trading Facility Operator and the facilities operated by it.

### 2.6.3. List of Members and Clients

A Digital Asset Trading Facility Operator must be able to provide the AFSA with a list of Members and Clients of its facility on the AFSA's request.

### 2.6.4. Undertaking to comply with AFSA rules

A Digital Asset Trading Facility Operator may not admit a Recognised Non-AIFC Member as a Member unless:

(a) the Recognised Non-AIFC Member agrees in writing to submit unconditionally to the jurisdiction of the AFSA in relation to any matters which arise out of or which relate to its use of the facility of the Digital Asset Trading Facility Operator;

(b) the Recognised Non-AIFC Member agrees in writing to submit unconditionally to the jurisdiction of the AIFC Court in relation to any disputes, or other proceedings in the AIFC, which arise out of or relate to its use of the facility of the Digital Asset Trading Facility Operator;

(c) the Recognised Non-AIFC Member agrees in writing to subject itself to the Acting Law of the AIFC in relation to its use of the facility of the Digital Asset Trading Facility Operator; and

(d) where the Recognised Non-AIFC Member is incorporated outside the Republic of Kazakhstan, appoints and maintains at all times, an agent for service of process in the AIFC.

## 2.7. Direct Electronic Access

### 2.7.1. Direct Electronic Access to the facility

For the purposes of these Rules, Direct Electronic Access means any arrangement, such as the use of the Member's trading code, through which a Member or the Clients of that Member are able to transmit electronically orders relating to Digital Assets directly to the facility provided by the Digital Asset Trading Facility Operator and includes arrangements which involve the use by a Person of the infrastructure of the Digital Asset Trading Facility Operator or the Member or Client or any connecting system provided by the Digital Asset Trading Facility Operator or Member or Client, to transmit the orders and arrangements where such an infrastructure is not used by a Person.

**Guidance:**

A Person who is permitted to have Direct Electronic Access to a Digital Asset Trading Facility Operator's facility through a Member is not, by virtue of such permission, a Member of the Digital Asset Trading Facility Operator.

### 2.7.2. Permitting Members that are Body Corporates to provide Direct Electronic Access to Clients

(1) This rule applies if a Digital Asset Trading Facility Operator proposes to permit a Member that is a Body Corporate to provide its Clients Direct Electronic Access to the Digital Asset Trading Facility Operator's facility.

(2) A Digital Asset Trading Facility Operator may permit a Member to provide its Clients Direct Electronic Access to the Digital Asset Trading Facility Operator's facility only if:

(a) the Clients meet the suitability criteria established by the Member in order to meet the requirements in DAA 2.7.3;

(b) the Member retains responsibility for the orders and trades executed by its Clients who are using Direct Electronic Access; and

(c) the Member has adequate mechanisms to prevent its Clients placing or executing orders using Direct Electronic Access in a manner that would result in the Member exceeding its position or margin limits.

### 2.7.3. Criteria, standards and arrangements for providing Direct Electronic Access to Clients of Members that are Body Corporates

(1) A Digital Asset Trading Facility Operator which permits its Members to provide its Clients Direct Electronic Access to the Digital Asset Trading Facility Operator's facility under DAA 2.7.2. must:

(a) set appropriate standards regarding risk controls and thresholds on trading through Direct Electronic Access;

(b) be able to identify orders and trades made through Direct Electronic Access; and

(c) if necessary, be able to stop orders or trades made by a Client using Direct Electronic Access provided by the Member without affecting the other orders or trades made or executed by that Member.

(2) A Client who is permitted to have Direct Electronic Access to a Digital Asset Trading Facility Operator's facility through a Member is not, by virtue of such permission, a Member of the Digital Asset Trading Facility Operator. However, such Client is subject to the jurisdiction of the Digital Asset Trading Facility Operator.

(3) In determining whether a Digital Asset Trading Facility Operator has adequate arrangements to permit Direct Electronic Access to its facility and to prevent and resolve problems likely to arise from the use of electronic systems to provide indirect access to its facility to Persons other than the Digital Asset Trading Facility Operator's Members, the AFSA may have regard to:

(a) the rules and guidance governing Members' procedures, controls and security arrangements for inputting instructions into the system;

(b) the rules and guidance governing the facilities that Members provide to their Clients to input instructions into the system and the restrictions placed on the use of those systems;

(c) the rules and practices to detect, identify, and halt or remove instructions breaching any relevant restrictions;

(d) the quality and completeness of the audit trail of a transaction processed through an electronic connection system;

(e) the systems and controls in place to monitor compliance with applicable law and regulation, cybersecurity requirements, as well as prevention of money laundering, Market Abuse and other Financial Crime; and

(f) the procedures in place to determine whether to suspend trading by Direct Electronic Access systems generally or access to those systems by or through individual Members.

### 2.7.4. Criteria, standards and arrangements for giving Direct Electronic Access to Members who are individuals (natural persons)

(1) This rule applies if a Digital Asset Trading Facility Operator proposes to give to a Member who is an individual (natural person) Direct Electronic Access to the Digital Asset Trading Facility Operator's facility.

(2) A Digital Asset Trading Facility Operator must ensure that:

(a) its rules clearly set out:

(i) the duties owed by the Digital Asset Trading Facility Operator to its Members with Direct Electronic Access, and how the Digital Asset Trading Facility Operator is held accountable for any failure to fulfil those duties; and

(ii) the duties owed by the Members with Direct Electronic Access to the Digital Asset Trading Facility Operator and how such Members are held accountable for any failure to fulfil those duties;

(b) appropriate investor redress mechanisms are available, in accordance with COB Chapter 15, and disclosed to Members permitted to trade Digital Assets on its facility; and

(c) its facility contains a prominent disclosure of the risks associated with trading and clearing Digital Assets.

(3) Without limiting the generality of the systems and controls obligations of the Digital Asset Trading Facility Operator, the Digital Asset Trading Facility Operator must have adequate systems and controls to address market integrity, AML and CTF, and investor protection risks in giving Direct Electronic Access to a Member, to trade on its facility, including procedures to:

(a) ensure that appropriate customer due diligence sufficient to address AML and CTF risks has been conducted on each Member, before permitting the Member to trade on its facility, and that such due diligence is updated periodically on an ongoing basis, and at least quarterly, after the establishment of relations with a Member;

(b) detect and address potential market manipulation and abuse; and

(c) ensure that there is adequate disclosure relating to the Digital Assets that are traded on the facility, including as regards any particular risks in relation to such.

(4) A Digital Asset Trading Facility Operator must maintain written policies and procedures to evidence compliance with the requirements of DAA 2.7.4(3).

(5) A Digital Asset Trading Facility Operator must have adequate controls and procedures to ensure that trading Digital Assets by Members with Direct Electronic Access does not pose any risks to the orderly and efficient functioning of the facility's trading system, including controls and procedures to:

(a) mitigate counterparty risks that may arise from defaults by such Members through adequate collateral management measures, such as margin requirements, based on the settlement cycle adopted by the Digital Asset Trading Facility Operator;

(b) identify and distinguish orders that are placed by such Members, and, if necessary, enable the Digital Asset Trading Facility Operator to stop orders of, or trading by, such Members;

(c) prevent such Members from allowing access to unauthorised Persons to trade on the trading facility; and

(d) ensure that such Members fully comply with the rules of the facility and promptly address any gaps and deficiencies that are identified.

(6) A Digital Asset Trading Facility Operator must have adequate resources and systems to carry out frontline monitoring of the trading activities of Members with Direct Electronic Access.

## 2.8. Admission of Digital Assets to trading

### 2.8.1. Application for admission of Digital Assets to trading

(1) Applications for the admission of a Digital Asset to trading can be made to a Digital Asset Trading Facility Operator by:

(a) an issuer of a Digital Asset;

(b) a third party on behalf of and with the consent of an issuer of a Digital Asset; or

(c) a Member of the Digital Asset Trading Facility Operator.

(2) A Digital Asset can be admitted to trading on the Digital Asset Trading Facility Operator's own initiative.

(3) A Digital Asset Trading Facility Operator must, before admitting any Digital Asset to trading:

(a) be satisfied that the applicable requirements, including those in its Admission to Trading Rules, have been or will be fully complied with in respect of such Digital Asset; and

(b) obtain approval of the AFSA in respect of Fiat and Commodity stablecoins, except for stablecoins issued by the Digital Asset Service Providers holding the relevant Licence.

(4) For the purposes of (1), a Digital Asset Trading Facility Operator must notify an applicant in writing of its decision in relation to the application for admission of the Digital Asset to trading.

(5) For the purposes of 3(b), an application to the AFSA by a Digital Asset Trading Facility Operator must include:

(a) a copy of the admission application; and

(b) any other information requested by the AFSA.

### 2.8.2. Admission criteria

(1) For the purposes of 2.8.1(3)(b), a Digital Asset can be admitted to trading on the Operator's facility if the Digital Asset Trading Facility Operator is satisfied that:

(a) having considered the matters in (2), the Digital Asset is suitable for use in the AIFC;

(b) the Digital Asset is not prohibited for use in the AIFC; and

(c) for a Fiat or Commodity stablecoin, all of the requirements in (4) or (5) as applicable are met in respect of that Fiat or Commodity stablecoin (and conditions (a) and (b) above are met).

(2) The matters referred to in (1)(a), which the Digital Asset Trading Facility Operator considers, are:

(a) the regulatory status of the relevant Digital Asset in other jurisdictions, including whether it has been assessed or approved for use in another jurisdiction, and the extent to which the laws and regulations of that jurisdiction are equivalent to the requirements of the AFSA;

(b) whether there is adequate transparency relating to the Digital Asset and underlying blockchain, including sufficient detail about its purpose, protocols, consensus mechanism, governance arrangements, founders, key persons, miners and significant holders;

(c) the size (the market capitalisation), liquidity and volatility of the market for the Digital Asset globally;

(d) whether there is a total limit (cap) for the issuance of Digital Asset;

(e) the controls/processes to manage volatility of a particular Digital Asset (tokenomics);

(f) the adequacy and suitability of the technology used in connection with the Digital Asset; and

(g) whether risks associated with the Digital Asset are adequately mitigated, including risks relating to governance, legal and regulatory issues, cybersecurity, money laundering, Market Abuse and other Financial Crime;

(h) whether a Digital Asset is traceable;

(i) whether there are any issues relating to the security or usability of a DLT used for the purposes of a Digital Asset; and

(j) whether a DLT and smart contract (if any) have been stress tested or subject to independent audit.

(3) In assessing the matters in (2), the AFSA may consider the cumulative effect of factors which, if taken individually, may be regarded as insufficient to give reasonable cause to doubt that the criteria in (1)(a) is satisfied.

(4) In the case of a Fiat stablecoin or Commodity stablecoin backed by a reserve, the additional criteria referred to in (1)(c) are that:

(a) information is published at least quarterly on the value and composition of the reserves backing the Fiat stablecoin or Commodity stablecoin;

(b) the published information referred to in (4)(a) is verified by a suitably qualified third-party professional who is independent of the issuer of the Digital Asset and any persons responsible for the Digital Asset;

(c) the published information referred to in (4)(a) demonstrates that the reserves in respect of Fiat stablecoins:

(i) are at least equal in value to the notional value of outstanding Digital Assets in circulation (that value being calculated by multiplying the number of Digital Assets in circulation by the purported pegged Fiat Currency value);

(ii) are denominated in the reference currency; and

(iii) are held in segregated accounts with properly regulated banks or custodians in jurisdictions with regulation that is equivalent to the AFSA's regime and AML regulation that is equivalent to the standards set out in the FATF Recommendations;

(d) the Digital Asset is able to maintain a stable price relative to the Fiat Currency or Commodity stablecoin it references; and

(e) a Person is clearly responsible and liable to investors for the Digital Asset.

(5) If a Digital Asset Trading Facility Operator decides to admit a Digital Asset to trading, the Digital Asset Trading Facility Operator is required to notify the AFSA 10 days prior to the date of the admission of the Digital Asset to trading.

### 2.8.3. Events or developments affecting the Digital Asset

(1) If a Digital Asset Trading Facility Operator becomes aware of any significant event or development that reasonably suggests that the Digital Asset no longer meets the criteria in DAA 2.8.2 for it to be admitted to trading, it must immediately suspend or withdraw a Digital Asset from trading.

(2) A Digital Asset Trading Facility Operator must ensure that, where it seeks to offer services in relation to the Digital Asset associated with the new version of an underlying protocol ("hard fork"), this new Digital Asset meets the requirements in DAA 2.8.2.

### 2.8.4. Publication of key features document

(1) A Digital Asset Trading Facility Operator may permit a Digital Asset to trading only if it has published a key features document on its website about the Digital Asset.

(2) The key features document must include the following if known (or, if not known, after having taken reasonable steps to determine this information, a clear statement must be provided that such information is not known):

(a) information about the issuer and the individuals responsible for designing the Digital Asset;

(b) characteristics of the Digital Asset, including rights attaching to the Digital Asset and any project or venture to be funded in connection with the Digital Asset (if relevant);

(c) details of Persons responsible for performing obligations associated with the Digital Asset and details of where and against whom rights conferred by the Digital Asset may be exercised;

(d) information on the underlying DLT or similar technology used for the Digital Asset, including details of the technology that is used to issue, store or transfer the Digital Asset and any interoperability with other DLT;

(e) information on the underlying technology used by the Digital Asset Trading Facility Operator, as relevant to making a decision to participate in the Digital Asset, including information on relevant protocols and technical standards adhered to;

(f) details about how ownership of the Digital Asset is established, certified or otherwise evidenced (to the extent relevant);

(g) how the Digital Asset will be valued by the Digital Asset Trading Facility Operator, and an explanation of how this is carried out and what benchmarks, indices or third parties relied on;

(h) the risks relating to the volatility and unpredictability of the price of the Digital Asset;

(i) in the case of a Fiat stablecoin or Commodity stablecoin based on reserves, details about the reserves backing that Fiat stablecoin or Commodity stablecoin and the stabilisation and redemption mechanisms;

(j) cyber-security risks associated with the Digital Asset or its underlying technology, including whether there is a risk of loss of the Digital Asset in the event of a cyberattack, and details of steps that have been taken, or can be taken, to mitigate those risks;

(k) the risks relating to fraud, hacking and Financial Crime;

(l) any other information relevant to the Digital Asset that would reasonably assist the Client to understand the Digital Asset and whether to participate in the Digital Asset, or otherwise use the service(s) being offered to the Client.

**Guidance:**

The Digital Asset white paper is a document outlining the main economic and technical aspects of a specific Digital Asset. The key features document is a document outlining the main characteristics of the Digital Asset in a simple format to provide potential investors with the aims and benefits of the Digital Asset, along with the relevant risks and limitations. The content of the Digital Asset white paper and key features document should not conflict each other.

### 2.8.5. Risk warnings

(1) A Digital Asset Trading Facility Operator must display prominently on its website the following risk warnings relating to Digital Assets:

(a) (except in the case of a Central Bank Digital Currency) that Digital Assets are not legal tender or backed by a government;

(b) that Digital Assets are subject to extreme volatility and the value of the Digital Asset can fall quickly (including, in respect of a stablecoin, if it loses its stability peg);

(c) that an investor in Digital Assets may lose all, or part, of the value of their investment;

(d) that Digital Assets may not always be liquid or transferable;

(e) that investments in Digital Assets may be complex making it hard to understand the risks associated with participating in them;

(f) that Digital Assets can be stolen because of cyber attacks;

(g) that trading in Digital Assets is susceptible to irrational market forces;

(h) there being limited or, in some cases, no mechanisms for the recovery of lost or stolen Digital Assets;

(i) the risks of Digital Assets with regard to anonymity, irreversibility of transactions, accidental transactions, transaction recording, and settlement;

(j) that the nature of Digital Assets means that technological difficulties experienced by the Digital Asset Trading Facility Operator or relevant Member may prevent access to or use of a Client's Digital Assets;

(k) that participating in Digital Assets is not comparable to participating in traditional investments such as Securities; and

(l) that there is no recognised compensation scheme to provide an avenue of redress for aggrieved participants.

(2) Where a Digital Asset Trading Facility Operator presents any marketing or educational materials and other communications relating to a Digital Asset on a website, in the general media or as part of a distribution made to existing or potential new Clients, it must include the risk warning referred to in DAA 2.8.5 (1) in a prominent place at or near the top of each page of the materials or communication.

(3) If the material referred to in DAA 2.8.5 (1) is provided on a website or an application that can be downloaded to a mobile device, the warning must be:

(a) statically fixed and visible at the top of the screen even when a person scrolls up or down the webpage; and

(b) included on each linked webpage on the website.

### 2.8.6. Undertaking to comply with the Acting Law of the AIFC

A Digital Asset Trading Facility Operator may not admit a Digital Asset to trading unless the Person who seeks to have Digital Assets admitted to trading:

(a) gives an enforceable undertaking to the AFSA to submit unconditionally to the jurisdiction of the AIFC in relation to any matters which arise out of or which relate to its use of the facilities of the Digital Asset Trading Facility Operator;

(b) agrees in writing to submit unconditionally to the jurisdiction of the AIFC Court in relation to any disputes, or other proceedings in the AIFC, which arise out of or relate to its use of the facilities of the Digital Asset Trading Facility Operator; and

(c) agrees in writing to subject itself to the Acting Law of the AIFC in relation to its use of the facilities of the Digital Asset Trading Facility Operator.

### 2.8.7. Review of compliance

The Digital Asset Trading Facility Operator must maintain arrangements to semi-annually review whether the Digital Assets admitted to trading on its facilities comply with the Admission to Trading Rules.

### 2.8.8. Admission of Digital Asset Derivatives

(1) A Digital Asset Trading Facility Operator may admit Digital Asset Derivatives to trading if it has obtained the AFSA's approval to do so.

(2) The AFSA may grant its approval under (1) only if it is satisfied that a Digital Asset Trading Facility Operator has appropriate systems and controls and policies and procedures to determine the appropriateness of Retail Clients to be offered Digital Asset Derivatives.

(3) A Digital Asset Trading Facility Operator that intends to offer Digital Asset Derivatives to Retail Clients must carry out an appropriateness test of a Retail Client and form a reasonable view that the Retail Client has:

(a) adequate skills and expertise to understand the risks involved in trading Digital Asset Derivatives; and

(b) the ability to absorb potentially significant losses resulting from trading in Digital Asset Derivatives.

(4) A Digital Asset Trading Facility Operator must maintain records of the appropriateness test that it carries out in respect of each Retail Client and make such records available to the AFSA on request.

(5) If it considers appropriate, the AFSA may restrict or prohibit the trading of Digital Asset Derivatives for certain types of Clients.

**Guidance:**

(1) To form a reasonable view referred to in DAA 2.8.8.(3) in relation to a Person, a Digital Asset Trading Facility Operator should consider issues such as whether the Person:

(a) has sufficient knowledge and experience relating to the type of a Digital Asset Derivative offered, having regard to such factors as:

(i) how often and in what volumes that Person has traded in the relevant type of a Digital Asset Derivative; and

(ii) the Person's relevant qualifications, profession or former profession;

(b) understands the characteristics and risks relating to Digital Asset Derivatives, and the volatility of the prices of Digital Asset Derivatives;

(c) understands the potential impact of leverage, due to which, there is potential to make significant losses in trading in Digital Asset Derivatives; and

(d) has the ability, particularly in terms of net assets and liquidity available to the Person, to absorb and manage any losses that may result from trading in the Digital Asset Derivatives offered.

(2) To be able to demonstrate to the AFSA that it complies with DAA 2.8.8.(3), a Digital Asset Trading Facility Operator should have in place systems and controls that include:

(a) pre-determined and clear criteria against which a Retail Client's ability to trade in Digital Asset Derivatives can be assessed;

(b) adequate records to demonstrate that the Digital Asset Trading Facility Operator has undertaken the appropriateness test for each Retail Client; and

(c) in the case of an existing Retail Client with whom the Digital Asset Trading Facility Operator has previously traded in Digital Asset Derivatives, procedures to undertake a fresh appropriateness test on at least an annual basis, and if:

(i) a new Digital Asset Derivative with a materially different risk profile is offered to the Retail Client; or

(ii) there has been a material change in the Retail Client's circumstances.

(3) If a Digital Asset Trading Facility Operator forms the view that it is not appropriate for a Person to trade in Digital Asset Derivatives, the Digital Asset Trading Facility Operator should refrain from offering that service to the Person. As a matter of good practice, the Digital Asset Trading Facility Operator should inform the Person of such decision.

## 2.9. Suspending or removing Digital Assets from trading

### 2.9.1. Power to suspend or remove a Digital Asset from trading

(1) The rules of a Digital Asset Trading Facility Operator must provide that it has the power to suspend or remove from trading on its facility any Digital Assets with immediate effect or from such date and time as may be specified where it is satisfied that there are circumstances that warrant such action, or it is in the interests of the AIFC.

(2) The AFSA may direct a Digital Asset Trading Facility Operator to suspend or remove Digital Assets from trading with immediate effect or from such date and time as may be specified by the AFSA if it is satisfied there are circumstances that:

(a) warrant such action, or

(b) it is in the interests of the AIFC.

(3) The AFSA may withdraw a direction made under (2) at any time.

(4) Digital Assets that are suspended from trading must remain admitted to trading for the purposes of this Chapter.

(5) The AFSA may prescribe any additional requirements or procedures relating to the removal or suspension of Digital Assets from or restoration of Digital Assets to trading.

### 2.9.2. Limitation on power to suspend or remove Digital Assets from trading

The rules of a Digital Asset Trading Facility Operator must contain provisions for orderly suspension and removal from trading on its facility of any Digital Asset which no longer complies with its rules, considering the interests of investors and the orderly functioning of the financial market of the AIFC.

### 2.9.3. Publication of decision

(1) Where the Digital Asset Trading Facility Operator suspends or removes any Digital Asset from trading on its facility, it must notify the AFSA in advance and make that decision public by issuing a public notice on its website.

(2) Where the Digital Asset Trading Facility Operator lifts a suspension or re-admits any Digital Asset to trading on its facility, it must notify the AFSA in advance and make that decision public by issuing a public notice on its website.

(3) Where a Digital Asset Trading Facility Operator has made any decisions on admission, suspension, or removal of Digital Assets from trading on its facility, it must have adequate procedures for notifying Members and Clients of such decisions.

## 2.10. Transparency obligations

### 2.10.1. Pre-trade disclosure

(1) A Digital Asset Trading Facility Operator must disclose to its Members and Clients the following information relating to trading of Digital Assets on its facility:

(a) the current bid and offer prices, and volume of Digital Assets traded on its systems on a continuous basis during normal trading hours;

(b) the depth of trading interest shown at the prices and volumes advertised through its systems for the Digital Assets;

(c) the methods of communication to be used between the Digital Asset Trading Facility Operator and its Members and Clients;

(d) the languages in which the Digital Asset Trading Facility Operator and its Members and Clients may communicate;

(e) a statement that the Digital Asset Trading Facility Operator has the appropriate Licence to operate, and the details of that Licence;

(f) a description, which may be in summary form, of any conflicts of interest which may arise in relation to potential transaction, and how the Digital Asset Trading Facility Operator will manage these to ensure the fair treatment of Members and Clients;

(g) any cancellation or withdrawal rights that Members and Clients may have;

(h) any rights of Members and Clients may or may not have to terminate a trade early or unilaterally under the terms of the Digital Asset Trading Facility Operator's facilities, including whether any fees or costs may be imposed in connection with exercising such a right;

(i) any specific technological requirements that the Members and Clients must have in place in order to use the Digital Asset Trading Facility; and

(j) any other information relating to Digital Assets which would materially promote transparency for Members and Clients relating to trading.

(2) The AFSA may waive or modify the disclosure requirement in DAA 2.10.1 (a) and (b) in relation to certain transactions where the order size is predetermined, exceeds a pre-set and published threshold level and details of the exemption are made available to the Digital Asset Trading Facility Operator's Members and the public.

(3) In assessing whether an exemption from pre-trade disclosure is allowed in relation to in DAA 2.10.1 (a) and (b), the AFSA would regard to such factors as:

(a) the level of an order threshold compared with the normal market size for the Digital Asset;

(b) the impact such an exemption would have on price discovery, fragmentation, fairness and overall market quality;

(c) whether there is sufficient transparency relating to trades executed without pre-trade disclosure (as a result of orders executed on execution platforms without pre-trade transparency), whether or not they are entered in transparent markets;

(d) whether the Digital Asset Trading Facility Operator supports transparent orders by giving a priority to transparent orders over dark orders, for example, by executing such orders at the same price as transparent orders; and

(e) whether there is adequate disclosure of details relating to dark orders available to Members and other participants on the Digital Asset Trading Facility to enable them to understand the manner in which their orders are handled and executed on the Digital Asset Trading Facility.

(4) When making disclosure, a Digital Asset Trading Facility Operator must adopt a technical mechanism showing differentiations between transactions that have been recorded in the central order book and transactions that have been reported to the Digital Asset Trading Facility as off-order book transactions. Any transactions that have been cancelled pursuant to its rules must also be identifiable.

(5) A Digital Asset Trading Facility Operator must use appropriate mechanisms to enable pre-trade information to be made available to Members and Clients in an easy to access and uninterrupted manner at least during normal trading hours.

### 2.10.2. Post-Trade Disclosure

(1) A Digital Asset Trading Facility Operator must disclose the price, volume and time of the transactions effected in respect of Digital Assets to Members and Clients involved in the relevant transaction as close to real-time as is technically possible on a non-discretionary basis. The Digital Asset Trading Facility Operator must use adequate mechanisms to enable post-trade information to be made available to Members and Clients involved in the relevant transaction in an easy to access and uninterrupted manner at least during business hours.

(2) A Digital Asset Trading Facility Operator must provide price, volume, time and counterparty details to the AFSA within 24 hours of the close of each trading day via a secure electronic feed.

### 2.10.3. Public notice of suspended or terminated Membership

The Digital Asset Trading Facility Operator must promptly issue a public notice on its website in respect of any Member that has a Licence to carry out the Regulated Activities whose Membership is suspended or terminated.

### 2.10.4. Cooperation with office-holder

The Digital Asset Trading Facility Operator must cooperate, by the sharing of information and otherwise, with the AFSA, any relevant office-holder and any other authority or body having responsibility for any matter arising out of, or connected with, the default of a Member of the Digital Asset Trading Facility Operator.

### 2.10.5. Forums

If a Digital Asset trading Facility Operator provides a means of communication (a "forum") for Members and Clients to discuss Digital Assets, it must:

(a) include a clear and prominent warning on the forum informing Members and Clients that the Digital Asset Trading Facility Operator does not conduct due diligence on information on the forum;

(b) restrict the posting of comments on the forum to Digital Asset Trading Facility Members and Clients;

(c) ensure that all Members and Clients of the forum have equal access to information posted on the forum;

(d) require a person posting a comment on the forum to disclose clearly if he is affiliated in any way with a Digital Asset or is being compensated, directly or indirectly, to promote a Digital Asset;

(e) take reasonable steps to monitor and prevent posts on the forum that are potentially misleading or fraudulent or may contravene the Market Abuse provisions (Chapter 5 of the MAR);

(f) immediately take steps to remove a post, or to require a post to be deleted or amended, if the Digital Asset Trading Facility Operator becomes aware that (d) or (e) have not been complied with; and

(g) not participate in discussions on the forum except to moderate posts or to take steps referred to in (f).

## 2.11. Clients

### 2.11.1. Clients of a Digital Asset Trading Facility Operator

Members of a Digital Asset Trading Facility Operator and their clients are Clients of a Digital Asset Trading Facility Operator.

### 2.11.2. Investment limits

A Digital Asset Trading Facility Operator must maintain effective systems and controls to ensure that a Retail Client, who is a resident of the Republic of Kazakhstan, complies with any

requirements and limits imposed by the Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC.

### 2.11.3. Calculation of an individual Client's net assets

(1) For the purposes of calculating an individual Client's net assets to treat him as an Assessed Professional Client under Rule 2.5.1(a) of the COB, the Digital Asset Trading Facility Operator:

(a) must exclude the value of the primary residence of the Client;

(b) must exclude Digital Assets belonging to the Client that are not admitted to trading;

(c) must include only 30% of the market value of a Digital Asset admitted to trading, which belongs to the Client, but must include 100% of the market value of Fiat and Commodity stablecoin backed by reserves, which belong to the Client; and

(d) may include any other assets held directly or indirectly by that Client.

### 2.11.4. Additional information for Providing Custody of Digital Assets

A Digital Asset Trading Facility Operator Providing Custody of Digital Assets must include in the Client Agreement:

(a) a breakdown of all fees and charges payable for a transfer of Digital Assets (a "transfer") and when they are charged;

(b) the information required to carry out a transfer;

(c) the form and procedures for giving consent to a transfer;

(d) an indication of the time it will normally take to carry out a transfer;

(e) details of when a transfer will be considered to be complete;

(f) how, and in what form, information and communications relating to transfer services will be provided to the Client, including the timing and frequency of communications and the language used and technical requirements for the Client's equipment and software to receive the communications;

(g) clear policies and procedures relating to unauthorised or incorrectly executed transfers, including when the Client is and is not entitled to redress;

(h) clear policies and procedures relating to situations where the holding or transfer of Digital Assets may have been compromised, such as if there has been hacking, theft or fraud; and

(i) details of the procedures the Digital Asset Trading Facility Operator will follow to contact the Client if there has been suspected or actual hacking, theft or fraud.

### 2.11.5. Provision of prompt confirmation to Clients

(1) Prior to execution of each transaction in Digital Assets, a Digital Asset Trading Facility Operator must confirm with its Clients the following terms:

(a) name of the Digital Asset in the proposed transaction, as well as any other identifying details required to be clear of the exact version of the Digital Asset subject to the proposed transaction;

(b) amount or value of the proposed transaction;

(c) fees and charges to be borne by the Client that are charged by or via the Digital Asset Trading Facility Operator, including applicable exchange rates; and

(d) a warning that once executed the transaction may not be undone.

(2) After a Digital Asset Trading Facility Operator has effected a transaction for a Client, it must confirm promptly with the Client the essential features of the transaction. The following information should be included:

(a) name of the Digital Asset in the transaction, as well as any other identifying details required to be clear of the exact version of the Digital Asset;

(b) amount or value of the transaction; and

(c) fees and charges borne by the Client that are charged by or via the Digital Asset Trading Facility Operator, including applicable exchange rates.

### 2.11.6. Provision of statements of account on request

If a Digital Asset Trading Facility Operator receives a request from a Client for a statement of account it must:

(a) prepare a statement of account in respect of the Client which includes the following information:

(i) the name, address and account number of the Client to whom the Digital Asset Trading Facility Operator is required to provide the statement of account;

(ii) the date on which the statement of account is prepared;

(iii) the outstanding balance of that account; and

(iv) the quantity, and, in so far as readily ascertainable, the market price and market value of each Client Digital Asset, held for that account.

(b) prepare the requested statement of account to the Client as soon as practicable after the date of the request.

## 2.12. Conflicts of interest

### 2.12.1. Conflicts of interest – core obligation

A Digital Asset Trading Facility Operator must take reasonable steps, including the maintenance of adequate systems and controls, governance and internal policies and procedures, to ensure that the performance of its regulatory functions and obligations is not adversely affected by its commercial interests.

**Guidance: regulatory functions of a Digital Asset Trading Facility Operator**

The regulatory functions of a Digital Asset Trading Facility Operator include, as appropriate:

• its obligations to monitor and enforce compliance with its Business Rules, Admission to Trading Rules, and Membership Rules;

• its obligation to prevent, detect and report Market Abuse or Financial Crime, as well as to comply with applicable laws and regulations generally; and

• its obligations in respect of admission of Digital Assets to trading or to clearing.

### 2.12.2. Conflicts of interest – identification and management

For the purposes of compliance with DAA 2.12.1, a Digital Asset Trading Facility Operator must:

(a) identify conflicts between the interests of the Digital Asset Trading Facility Operator, its shareholders, owners and operators and the interests of the Persons who make use of its facilities operated by it; and

(b) manage and disclose such conflicts so as to avoid adverse consequences for the sound functioning and operation of the facilities operated by the Digital Asset Trading Facility Operator and for the Persons who make use of its them.

### 2.12.3. Personal account transactions

A Digital Asset Trading Facility Operator must establish and maintain adequate policies and procedures to ensure that its Employees do not undertake personal account transactions in Digital Assets in a manner that creates or has the potential to create conflicts of interest or otherwise create a risk of Market Abuse or Financial Crime.

### 2.12.4. Conflicts of interest – code of conduct

A Digital Asset Trading Facility Operator must establish a code of conduct that sets out the expected standards of behaviour for its Employees, including clear procedures for addressing (potential) conflicts of interest. Such a code must be binding on all of its Employees.

## 2.13. Other requirements and obligations

### 2.13.1. Measures to prevent, detect and report Market Abuse or Financial Crime

A Digital Asset Trading Facility Operator must:

(a) ensure that appropriate measures (including the monitoring of transactions effected on or through the Digital Asset Trading Facility Operator's facility) are adopted to reduce the extent to which the Digital Asset Trading Facility Operator's facility can be used for a purpose connected with Market Abuse, Financial Crime or money laundering, and to facilitate their detection and monitor their incidence; and

(b) immediately report to the AFSA any suspected Market Abuse, Financial Crime or money laundering, along with full details of that information in writing.

### 2.13.2. Whistleblowing

A Digital Asset Trading Facility Operator must have appropriate procedures and protections for its Employees to disclose any information to the AFSA in a manner which does not expose them to any disadvantage or discrimination as a result of so doing.

### 2.13.3. Lending and staking

(1) A Digital Asset Trading Facility Operator must not offer or provide any facility or service that allows a Member or another user of its facility to lend a Digital Asset to another Person unless it is reasonably satisfied that the Member or user is a Professional Client.

(2) The prohibition in (1) does not apply to the provision of any Digital Asset to an Authorised Firm as Collateral.

### 2.13.4. Trading of Digital Assets

(1) A Digital Asset Trading Facility Operator must establish and maintain policies and procedures relating to the trading process to detect and prevent (potential) errors, omissions, fraud, and other unauthorised or improper activities.

(2) A Digital Asset Trading Facility Operator must execute a trade for a Client only if there are sufficient Fiat Currencies or Digital Assets, which are admitted to trading, in the Client's account with the Digital Asset Trading Facility Operator to cover that trade. This requirement does not apply to any off-platform transactions to be conducted by institutional investors which are settled intra-day.

(3) A Digital Asset Trading Facility Operator should not provide any financial assistance for its Clients to acquire Digital Assets. It should ensure, to the extent possible, that no Person within the same Group as the Digital Asset Trading Facility Operator does so unless for exceptional circumstances which should be approved by the AFSA on a case-by-case basis.

### 2.13.5. Trading controls

(1) A Digital Asset Trading Facility Operator must put in place risk management and supervisory controls for the operation of its trading platform. These controls should include:

(a) automated pre-trade controls that are reasonably designed to:

(i) prevent the entry of any orders that would exceed appropriate position limits prescribed for each Member and Client;

(ii) alert the user to the entry of potential erroneous orders and prevent the entry of erroneous orders;

(iii) prevent the entry of orders which are not in compliance with regulatory requirements; and

(b) post-trade monitoring to reasonably identify any:

(i) suspicious market manipulative or abusive activities; and

(ii) market events or system deficiencies, such as unintended impact on the market, which call for further risk control measures.

(2) A Digital Asset Trading Facility Operator must be able to:

(a) reject orders that exceed its pre-determined volume and price thresholds, or that are clearly erroneous;

(b) temporarily halt or constrain trading on its facility if necessary or desirable to maintain an orderly market; and

(c) cancel, vary, or correct any order resulting from an erroneous order entry or the malfunctioning of the system of a Member.

### 2.13.6. Settlement and clearing arrangements

(1) A Digital Asset Trading Facility Operator must ensure that satisfactory arrangements are made for securing the timely discharge (whether by performance, compromise or otherwise), clearing and settlement of the rights and liabilities of the parties to transactions effected on the Digital Asset Trading Facility Operator's facilities (being rights and liabilities in relation to those transactions).

(2) A Digital Asset Trading Facility Operator must ensure that clearing and settlement of transactions on its facilities takes place only by means of Fiat Currencies or Digital Assets which are admitted to trading.

(3) A Digital Asset Trading Facility Operator must take all reasonable steps to ensure that finality of settlement is achieved within 24 hours.

### 2.13.7. Digital Asset Trading Facility Operator Providing Custody of Digital Assets

(1) A Digital Asset Trading Facility Operator which also carries out the Regulated Activity of Providing Custody of Digital Assets or Arranging Custody of Digital Assets must ensure that it complies with the requirements applicable to those Regulated Activities in addition to the requirements that apply by virtue of being a Digital Asset Trading Facility Operator.

(2) Digital Assets held by a Digital Asset Trading Facility Operator Providing Custody are not depository liabilities or assets of the Digital Asset Trading Facility Operator and must be held on trust.

(3) A Digital Asset Trading Facility Providing Custody must segregate the Digital Assets of each Client in separate Digital wallets containing the Digital Assets of that Client only.

(4) A Digital Asset Trading Facility Providing Custody must maintain control of each Digital Asset at all times while Providing Custody.

(5) A Digital Asset Trading Facility Operator Providing Custody must:

(a) have appropriate rules, procedures, and controls, including robust accounting practices, to safeguard the rights of Digital Assets issuers and holders, prevent the unauthorised creation or deletion of Digital Assets, and conduct daily reconciliation of each Digital Asset balance it maintains for issuers and holders;

(b) prohibit overdrafts and credit balances in Digital Assets account;

(c) maintain Digital Assets in an immobilised or dematerialised form for their transfer by book entry;

(d) protect assets against custody risk through appropriate rules and procedures consistent with its legal framework;

(e) ensure segregation between its own assets and the Digital Assets of its participants, as well as keeping clear records regarding which Digital Assets belong to which participant; and

(f) identify, measure, monitor, and manage its risks from other activities that it may perform.

(6) A Digital Asset Trading Facility Operator acting as a Digital Asset Custodian must have systems and procedures to enable segregation and portability of the Clients' assets.

(7) A Digital Asset Trading Facility Operator must:

(a) have segregation and portability arrangements to effectively protect the Clients' assets;

(b) structure portability arrangements in a way that ensures there is a high probability that the assets of one party will be transferred to another party; and

(c) disclose any constraints, including legal and operational constraints, that may impair its ability to segregate or port the Clients' assets.

### 2.13.8. Requirements for a Digital Asset Trading Facility Operator appointing a Third Party Digital wallet Service Provider

A Digital Asset Trading Facility Operator which appoints a Third Party Digital wallet Service Provider to provide custody of Digital Assets traded on its facility, must ensure that the Person is:

(1) an Authorised Firm appropriately authorised to be a Digital wallet Service Provider; or

(2) a Person which is appropriately regulated by a Financial Services Regulator to an equivalent level of regulation to that provided for under the AFSA regime for providing digital wallet services.

(3) When determining whether a Third Party wallet Service Provider is appropriate, the Digital Asset Trading Facility Operator must take into account:

(a) the expertise and reputation of the Third Party wallet Service Provider;

(b) the Third Party wallet Service Provider's performance of its services to the Digital Asset Trading Facility Operator;

(c) the arrangements the Third Party wallet Service Provider has in place for holding and safeguarding Digital Assets;

(d) the capital or financial resources of the Third Party wallet Service Provider;

(e) the credit-worthiness of the Third Party wallet Service Provider;

(f) any other activities carried out by the Third Party wallet Service Provider; and

(g) anything else that could adversely affect rights of Members and Clients.

(4) A Digital Asset Trading Facility Operator must conduct on a regular basis, and least once every 2 months, reconciliations between its internal records and accounts of Digital Assets and those held by the Third Party Digital wallet Service Provider.

(5) If a Digital Asset Trading Facility Operator appoints a Third Party Digital wallet Service Provider, the Digital Asset Trading Facility Operator must accept the same level of responsibility to its Members and Clients and AFSA as would be the case if the Digital Asset Trading Facility Operator were holding the relevant Digital Assets directly.

**Guidance:**

If a Digital Asset Trading Facility Operator appoints a non-AIFC firm regulated by a Financial Services Regulator, it must undertake sufficient due diligence to establish that the non-AIFC firm is subject to an equivalent level of regulation as under the AFSA regime in respect of that service.

### 2.13.9. Requirements in relation to Hot and Cold Digital wallets

A Digital Asset Trading Facility Operator must ensure that not more than 30 % of the Retail Client's Digital Assets are stored in Hot Digital wallets.

### 2.13.10. Obligation to report transactions

(1) A Digital Asset Trading Facility Operator must report to the AFSA details of transactions in Digital Assets traded on its facility which are executed, or reported, through its systems.

(2) The AFSA may, by written notice or guidance, specify:

(a) the information to be included in reports made under the preceding paragraph; and

(b) the manner in which such reports are to be made.

### 2.13.11. Obligation to report to the AFSA

(1) A Digital Asset Trading Facility Operator must submit to the AFSA a quarterly report that should include its financial statement, its income statement, a calculation of its relevant capital resources and a statement of its compliance and any non-compliance with these Rules.

(2) A Digital Asset Trading Facility Operator must provide the following information to the AFSA within 6 months after financial year end:

(a) the number of prospective clients which the Digital Asset Trading Facility Operator rejected during the reporting period;

(b) the number of Clients which were offboarded during the reporting period;

(c) the number of Clients where enhanced due diligence was applied;

(d) the total number of the Digital Asset Trading Facility Operator's Clients;

(e) the number of Clients originating from a high risk jurisdiction;

(f) the number of Clients on-boarded on a face-to-face basis;

(g) a description of any changes to the Client onboarding process;

(h) the number of suspicious transaction reports filed during the reporting period;

(i) the number of individuals supporting the MLRO;

(j) when the Digital Asset Trading Facility Operator's risk assessment was last updated and if there were any additional risks;

(j) (if applicable) the number of private keys held;

(k) (if applicable) whether Client's Digital Assets are held with a third party custodian;

(l) whether the Digital Asset Trading Facility Operator forms part of a Group, and if so, the Group structure;

(m) whether the Digital Asset Trading Facility Operator entered into any resource sharing agreements and, if so, the names of the counterparty/company;

(n) whether the Digital Asset Trading Facility Operator outsources any of its functions and, if so, any changes to the functions outsourced and to which companies;

(o) an overview of any involvement of the Digital Asset Trading Facility Operator's shareholders in the day-to-day operations of the Digital Asset Trading Facility Operator during the reporting period; and

(p) an overview of any instances of market abuse encountered by the Digital Asset Trading Facility Operator during the reporting period.

(3) The AFSA may request a Digital Asset Trading Facility to submit other returns. The AFSA from time to time may prescribe the required list of returns to be submitted and the returns templates to be used.

(4) Returns submitted to the AFSA must be signed by two (2) Approved Individuals and one of them must be approved to exercise the Finance Officer function.

### 2.13.12. Obligation to notify the AFSA

If a Digital Asset Trading Facility Operator becomes aware, or has a reasonable ground to believe, that it is or may be (or may be about to be) in breach of any of these Rules, it must:

(a) notify the AFSA in writing about the breach and the relevant circumstances immediately and not later than within 1 business day of becoming aware of it.

**Guidance:**

In dealing with a breach, or possible breach, of this part, the AFSA's primary concern will be the interests of existing and prospective members and clients, the potential adverse impact on market participants, and market stability. The AFSA recognises that there will be circumstances in which a problem may be resolved quickly, for example, by support from a parent entity, without jeopardising the interests of Members, Clients and other stakeholders. In such circumstances, it will be in the interests of all parties to minimise the disruption to the Digital Asset Trading facility Operator's business. The AFSA will normally seek to work cooperatively with the Digital

Asset Trading Facility Operator in stressed situations to deal with any problems. There will, however, be circumstances in which it is necessary to take regulatory action to avoid exposing market participants, Members, Clients and other stakeholders to the potential adverse consequences of the Digital Asset Trading Facility Operator's Failure, and the AFSA will not hesitate to take appropriate action if it considers this necessary.

## 2.14. Restrictions

### 2.14.1. Restriction on own account transactions

(1) A Digital Asset Trading Facility Operator or any of its Associates may not execute an Own Account Transaction in a Digital Asset if it is expected to materially affect the price of the Digital Asset.

(2) For the purposes of this Rule:

(a) "Own Account Transaction" means a transaction Executed for the Digital Asset Trading Facility Operator's own benefit or for the benefit of its Associate; and

(b) "Execute", in relation to a transaction, means carrying into effect or performing the transaction, whether as principal or as agent, including instructing another Person to execute the transaction.

(3) A Digital Asset Trading Facility Operator or any of its Associate must not use the Client's Digital Assets for their own account or the account of any other Person unless:

(a) the Client has given express prior consent to such use of the Digital Assets on specified terms; and

(b) the use of that Client's Digital Assets is restricted to the specified terms to which the Client consents.

### 2.14.2. Offer of incentives

If a Digital Asset Trading Facility Operator offers or provides to a Retail Client any incentive that influences, or is reasonably likely to influence, the Retail Client to trade in a Digital Asset or Digital Asset Derivative, it must comply with the requirements set out in Chapter 3 of the COB.

## 2.15. Prohibitions

### 2.15.1. Prohibition on use of Privacy Tokens and Privacy Devices

A Person must not in or from the AIFC:

(a) carry out a Regulated Activity relating to a Privacy Token or that involves the use of a Privacy Device;

(b) make or approve a Financial Promotion relating to a Privacy Token; or

(c) offer to the public a Privacy Token.

## 2.16. AFSA power to impose requirements

Without limiting the powers available to the AFSA under Part 8 of the Framework Regulations, the AFSA may direct an Authorised Market Institution to do or not do specified things that the

AFSA considers are necessary or desirable or to ensure the integrity of the AIFC financial markets, including but not limited to directions imposing on a Digital Asset Trading Facility Operator any additional requirements that the AFSA considers appropriate.

## 3. RULES APPLICABLE TO DIGITAL ASSET SERVICE PROVIDERS

This Part 3 applies to a Person carrying on, in or from the AIFC, one or more of the following Regulated Activities in relation to Digital Assets:

(a) Dealing in Investments as Principal;

(b) Dealing in Investments as Agent;

(c) Managing Investments;

(d) Managing a Collective Investment Scheme;

(e) Providing Custody;

(f) Arranging Custody;

(g) Advising on Investments; and

(h) Arranging Deals in Investments.

A Digital Asset Service Provider must incorporate into its internal documents the substance of additional provisions relevant to Derivatives to be found in the COB Rules, for the purpose of regulating operations in Digital Assets Derivatives.

### 3.1. Authorisation of Digital Asset Service Providers

A Person wishing to carry on one or more of the Regulated Activities in relation to Digital Assets in or from the AIFC must be an Authorised Firm licensed by the AFSA.

### 3.2. Requirements for Digital Asset Service Providers

(1) The AFSA may not grant authorisation or variation of a Licence to a Person to carry on the Regulated Activities in relation to Digital Assets unless the applicant satisfies all of the following requirements:

(a) general authorisation requirements applicable to the applicant under the Framework Regulations and other applicable rules, and

(b) the applicant must ensure that it maintains at all times capital resources in the amount specified in Table 2 by reference to the activity that the Digital Asset Service Provider is authorised to conduct or, if it is authorised to conduct more than one such activity, the amount that is the higher or highest of the relevant amounts in Table 2.

**Table 2**

| Regulated Activity | Capital requirement (USD) |
|---|---|
| Dealing in Investments as Principal, unless such activities are limited to matching client orders and the AFSA determines that it is appropriate in all the circumstances to apply a lower capital requirement | 250,000 |

| | |
|---|---|
| Dealing in Investments as Principal, where such activities are limited to matching client orders and the AFSA determines that it is appropriate in all the circumstances to apply a lower capital requirement than above | 50,000 |
| Dealing in Investments as Agent | 50,000 |
| Managing Investments | 100,000 |
| Managing a Collective Investment Scheme, which is an externally managed Exempt Fund and has an appointed Eligible Custodian (if an Eligible Custodian is required) | 50,000 |
| Managing a Collective Investment Scheme, which is a Non-Exempt Fund | 150,000 |
| Managing a Collective Investment Scheme, which does not have an appointed Eligible Custodian, except where an Eligible Custodian is not required due to the nature of the Fund and type of assets which it holds | 250,000 |
| Providing Custody | 250,000 |
| Arranging Custody | 10,000 |
| Advising on Investments | 10,000 |
| Arranging Deals in Investments | 10,000 |

(2) In determining whether a Digital Asset Service Provider meets the capital requirement(s) and, in particular, has sufficient working capital to continue business on a go-forwards basis, the Digital Asset Service Provider must have regard to the following matters:

(a) the business carried out, or to be carried out by the Digital Asset Service Provider;

(b) the risks to the continuity of the services provided by, or to be provided by, the Digital Asset Service Provider, including any outsourced services (including services outsourced to a Group entity where applicable);

(c) the liabilities to which the Digital Asset Service Provider is exposed or could be exposed to, including as a result of any failure by any third party; and

(d) the means by which the Digital Asset Service Provider manages and, if the Digital Asset Service Provider is a member of a Group, by which other members of the Group manage, the occurrence of risk in connection with the Digital Asset Service Provider's business.

**Guidance**

Intangible assets, including goodwill, cannot be used as part of determining whether the capital requirement value is met or whether the Digital Asset Service Provider has sufficient working capital, and must be disregarded when determining whether the requirements are met for the purposes of Table 2.

A Digital Asset Service Provider may carry on the Regulated Activities only in relation to Digital Assets and may not carry on the Regulated Activities in relation to other Investments unless for circumstances which could be approved by the AFSA on a case-by-case basis.

## 3.3. Governance

### 3.3.1. Mandatory appointments

(1) In addition to the mandatory appointments required by GEN 2.1., a Digital Asset Service Provider must appoint a Chief Information Technology Officer, who is an individual responsible for its ongoing information technology ("IT") operations, maintenance and security oversight to ensure that the Digital Asset Service Provider's IT systems are reliable and adequately protected from external attack or incident.

(2) AFSA may direct a Digital Asset Service Provider to appoint a Risk Manager.

### 3.3.2. Board of Directors of a Digital Asset Service Provider

(1) A Digital Asset Service Provider must have an effective Board of Directors which is collectively accountable for ensuring that the Digital Asset Service Provider's business is managed prudently and soundly. At least one-third of the Board of Directors should comprise independent Directors.

*Note: Rule 2.3.2(1) will come into force 12 months after the commencement of these Rules.*

(2) The AFSA may issue guidance on the requirements relating to Board composition, structure, duties and powers as well as skills, experience and qualifications of Directors, and other relevant requirements.

(3) The Board must ensure that there is a clear division between its responsibility for setting the strategic aims and undertaking the oversight of the Digital Asset Service Provider and the senior management's responsibility for managing the Digital Asset Service Provider's business in accordance with the strategic aims and risk parameters set by the Board as well as applicable law and regulation.

(4) The Board and its committees must have an appropriate balance of skills, experience, independence, and knowledge of the Digital Asset Service Provider's business, and adequate resources, including access to expertise as required and timely and comprehensive information relating to the affairs of the Digital Asset Service Provider.

(5) The Board must ensure that the Digital Asset Service Provider has an adequate, effective, well-defined and well-integrated risk management, internal control and compliance framework.

(6) The Board must ensure that the rights of shareholders are properly safeguarded through appropriate measures that enable the shareholders to exercise their rights effectively, promote effective dialogue with shareholders and other key stakeholders as appropriate, and prevent any abuse or oppression of minority shareholders.

(7) The Board must ensure that the Digital Asset Service Provider's financial and other reports present an accurate, balanced and understandable assessment of the Digital Asset Service

Provider's financial position and prospects by ensuring that there are effective internal risk control and reporting requirements.

(8) A Director of the Digital Asset Service Provider must act:

(a) on a fully informed basis;

(b) in good faith;

(c) honestly;

(d) with due skill, care and diligence; and

(e) in the best interests of the Digital Asset Service Provider and its shareholders and users.

### 3.4. Technology governance, controls and security

#### 3.4.1. Systems and controls

(1) A Digital Asset Service Provider must ensure that it implements systems and controls necessary to address the risks, including cybersecurity-related risks, to its business. The relevant systems and controls should take into account such factors that include but are not limited to the nature, scale and complexity of the Digital Asset Service Provider's business, the diversity of its operations, the volume and size of transactions made using its facilities and the level of risk inherent with its business and activities.

(2) A Digital Asset Service Provider must have adequate systems and controls to enable it to calculate and monitor its capital resources and its compliance with the requirements in DAA 3.2. The systems and controls must be in writing and must be appropriate for the nature, scale and complexity of the Digital Asset Service Provider's business and its risk profile.

#### 3.4.2. Technology governance and risk assessment framework

(1) A Digital Asset Service Provider must implement a technology governance and risk assessment framework which must be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in its business model.

(2) The technology governance and risk assessment framework must apply to all technologies relevant to a Digital Asset Service Provider's business and clearly set out the Digital Asset Service Provider's cybersecurity objectives, including the requirements for the competency of its relevant Employees and, as relevant, end users and Clients, and there must be in place clearly defined systems and procedures necessary for managing risks.

(3) A Digital Asset Service Provider must ensure that its technology governance and risk assessment is capable of determining the necessary processes and controls that it must implement in order to adequately mitigate any risks identified. In particular, a Digital Asset Service Provider must ensure that its technology governance and risk assessment framework includes consideration of international standards and industry best practice codes.

(4) A Digital Asset Service Provider must ensure that its technology governance and risk assessment framework incorporates appropriate governance policies and system development controls, such as a development, maintenance and testing process for technology systems and operations controls, back-up controls, capacity and performance planning and availability testing.

### 3.4.3. Cyber-security matters

A Digital Asset Service Provider must take reasonable steps to ensure that its IT systems are reliable and adequately protected from external attack or incident, as well as from risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems of third-party suppliers, agents and others). A Digital Asset Service Provider must ensure there are the necessary resources in place to manage these risks.

### 3.4.4. Cyber-security policy

(1) A Digital Asset Service Provider must create and implement a policy which outlines its procedures for the protection of its electronic systems.

(2) A Digital Asset Service Provider must ensure that its cyber-security policy is reviewed at least on an annual basis by its Chief Information Technology Officer, and that such review is provided to the Board of Directors.

(3) The cyber-security policy must, as a minimum, 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, consensus protocol methodology, code and smart contract validation and audit processes;

(h) systems and application development and quality assurance;

(i) physical security and environmental controls, including but not limited to procedures around access to premises and systems;

(j) customer data privacy;

(k) procedures regarding facilitation of Digital Asset transactions initiated by a Client including, but not limited to, considering multi-factor authentication or any better standard for Digital Asset transactions that—

(i) exceed transaction limits set by the Client, such as accumulative transaction limits over a period of time; and

(ii) are initiated after a material change of personal details by the Client, such as the address of a Digital wallet;

(l) procedures regarding Client authentication and session controls including, but not limited to, the maximum number of incorrect attempts permitted for entering a password, appropriate time-out controls and password validity periods;

(m) procedures establishing adequate authentication checks when a change to a Client's account information or contact details is requested;

(n) vendor and third-party service provider management;

(o) monitoring and implementing changes to core protocols not directly controlled by the Digital Asset Service Provider, as applicable;

(p) incident response, including but not limited to, root cause analysis and rectification activities to prevent reoccurrence;

(q) governance framework and escalation procedures for effective decision-making and proper management and control of risks and emergency incidents, including but not limited to responses to ransomware and other forms of cyberattacks; and

(r) hardware and infrastructure standards, including but not limited to network lockdown, services/desktop security and firewall standards.

(4) A Digital Asset Service Provider must consider the impact of any outsourcing arrangements, as well as the interoperability risks when dealing with systems and software provided by third parties, where applicable.

(5) A Digital Asset Service Provider must ensure all staff receive appropriate training in relation to cybersecurity.

(6) A Digital Asset Service Provider must inform the AFSA as soon as practicable if it becomes aware, or has reasonable grounds to believe, that a significant breach by any Person of its cyber-security may have occurred.

### 3.4.5. Cryptographic keys and Digital wallets management procedure

(1) A Digital Asset Service Provider must ensure that its cryptographic keys and Digital wallets management procedure addresses, to the extent necessary, the generation of cryptographic keys and Digital wallets, the signing and approval of transactions, the storage of cryptographic keys and seed phrases, and Digital wallets creation and management thereof.

(2) A Digital Asset Service Provider must:

(a) safeguard access to Digital Assets in accordance with industry best practices and, in particular, ensure that there is no single point of failure in the Digital Asset Service Provider's access to, or knowledge of, Digital Assets held by the Digital Asset Service Provider;

(b) adopt industry best practices for storing the private keys of Clients, including ensuring that keys stored online or in one physical location are not capable of being used to conduct a Digital Asset transaction, unless appropriate controls are in place to ensure that access by an unauthorised individual is insufficient to conduct a transaction;

(c) ensure that backups of the key and seed phrases are stored in a separate location from the primary key or seed phrase;

(d) adopt strict access management controls to manage access to keys, including an audit log detailing each change of access to keys; and

(e) adopt procedures designed to be able to immediately revoke a key signatory's access.

(3) A Digital Asset Service Provider must:

(a) ensure that the key generation process ensures that revoked signatories do not have access to the backup seed phrase or knowledge of the phrase used in the key's creation;

(b) perform internal audits on a quarterly basis concerning the removal of user access by reviewing access logs and verifying access as appropriate;

(c) implement and maintain a procedure for documenting the onboarding and offboarding of staff;

(d) implement and maintain a procedure for documenting a Digital Asset Service Provider's permission to grant or revoke access to each role in its key management system; and

(e) regularly assess the security of its IT systems or software integrations with external parties and ensure that the appropriate safeguards are implemented in order to mitigate all relevant risks.

(4) A Digital Asset Service Provider should provide information to Clients on measures they can take to protect their keys or seed phrases from misuse or unauthorised access, and the consequences of sharing their private keys and other security information.

(5) A Digital Asset Service Provider must ensure that access to its systems and data may only be granted to individuals with a demonstrable business need and implement safeguards to ensure the proper identification of all individuals, including the maintenance of an access log.

### 3.4.6. On-going monitoring

For the purposes of meeting the requirement in DAA 3.4.1, a Digital Asset Service Provider must have adequate procedures and arrangements for the evaluation, selection and on-going maintenance and monitoring of its IT systems. Such procedures and arrangements must, at a minimum, provide for:

(a) problem management and system change;

(b) testing IT systems before live operations in accordance with the requirements in DAA 3.4.7;

(c) real time monitoring and reporting on system performance, availability and integrity; and

(d) adequate measures to ensure:

(i) IT systems are resilient and not prone to failure;

(ii) business continuity in the event that an IT system fails;

(iii) protection of IT systems from damage, tampering, misuse or unauthorised access; and

(iv) the integrity of data forming part of, or being processed through, IT systems.

### 3.4.7. Testing and audit of technology systems

(1) A Digital Asset Service Provider must, before commencing live operation of its IT systems or any updates thereto, use development and testing methodologies in line with internationally accepted testing standards in order to test the viability and effectiveness of such systems. For this purpose, the testing must be adequate for the Digital Asset Service Provider to obtain reasonable assurance that, among other things:

(a) the systems enable it to comply with all the applicable requirements on an on-going basis;

(b) the systems can continue to operate effectively in stressed market conditions;

(c) the systems have sufficient electronic capacity to accommodate reasonably foreseeable volumes of messaging and orders; and

(d) any risk management controls embedded within the systems, such as generating automatic error reports, work as intended.

(2) A Digital Asset Service Provider must to undergo a qualified independent third-party technology governance and IT audit to conduct vulnerability assessments and penetration testing at least on an annual basis.

(3) A Digital Asset Service Provider must engage a qualified independent third-party auditor to audit any new systems, applications and products prior to their use.

(4) A Digital Asset Service Provider must provide the results of technology governance and IT assessments and tests to the AFSA promptly upon its request.

### 3.4.8. Technology audit reports

(1) This Rule applies to a Digital Asset Service Provider that:

(a) holds or controls Digital Assets;

(b) relies on DLT or similar technology to carry on one or more of the following Regulated Activities in relation to Digital Assets:

(i) Dealing in Investments as Principal;

(ii) Dealing in Investments as Agent;

(iii) Arranging Deals in Investments;

(iv) Managing Investments;

(v) Advising on Investments;

(vi) Providing Custody; or

(vii) Arranging Custody; or

(viii) is Managing a Collective Investment Scheme where 10% or more of the gross asset value of the Fund Property of the Fund consists of Digital Assets.

(2) The Authorised Firm must:

(a) appoint a suitably qualified independent third-party professional to:

(i) carry out an annual audit of the Authorised Firm's compliance with the technology resources and governance requirements that apply to it; and

(ii) produce a written report which sets out the methodology and results of that annual audit, confirms whether the requirements referred to in DAA 3.4.7 have been met and lists any recommendations or areas of concern;

(b) submit to the AFSA a copy of the report referred to in DAA 3.4.8. (2)(a)(ii) within 6 months of the financial year end; and

(c) be able to satisfy the AFSA that the independent third party professional appointed to carry out the annual audit has the relevant expertise to do so, and that the Authorised Firm has done proper due diligence to satisfy itself of that fact.

**Guidance:**

Credentials which indicate a qualified independent third-party auditor is suitable to conduct audit of technology governance and IT systems may include:

(1) designation as a Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM) by the Information Systems Audit and Control Association (ISACA);

(2) designation as a Certified Information Systems Security Professional (CISSP) by the International Information System Security Certification Consortium (ISC);

(3) accreditation by a recognised and reputable body to certify compliance with relevant ISO/IEC 27000 series standards; or

(4) accreditation by the relevant body to certify compliance with the Kazakhstani standards in the area of information (cyber) security.

## 3.5. Policies, procedures, and public disclosures

### 3.5.1. Policies and procedures required for Digital Asset Service Providers

(1) A Digital Asset Service Provider carrying out a Regulated Activity of Advising on Investments must establish, implement and enforce appropriate written internal policies and procedures relating to the following:

(a) how it ensures the independent basis of its advice;

(b) how it explains the range of Digital Assets considered in providing its advice;

(c) how it ensures all Directors and Employees providing the relevant advice are sufficiently competent; and

(d) such other policies and procedures as the AFSA may require from time to time.

(2) A Digital Asset Service Provider carrying out Regulated Activities of Dealing in Investments as Principal or Agent must establish, implement and enforce appropriate written internal policies and procedures relating to the following:

(a) the prohibition, detection, prevention or deterrence of market offences and any other abusive practices within their business or using their services including, but not limited to, relevant internal rules, compliance programmes, sanctioning policies and powers;

(b) Execution and routing of Client orders;

(c) the ability of Clients to have access to and withdraw their Digital Assets including, but not limited to, during periods of high uncertainty or extreme volatility; and

(d) such other policies and procedures as the AFSA may require from time to time.

(3) A Digital Asset Service Provider carrying out a Regulated Activity of Providing Custody must establish, implement and enforce appropriate written internal policies and procedures relating to the following:

(a) the ability of Clients to have access to and withdraw their Digital Assets including, but not limited to, during periods of high uncertainty or extreme volatility; and

(b) such other policies and procedures as the AFSA may require from time to time.

(4) A Digital Asset Service Provider carrying on a Regulated Activity of Managing Investments must establish, implement and enforce appropriate written internal policies and procedures relating to the following:

(a) the ability of Clients to have access to and withdraw their Digital Assets including, but not limited to, during periods of high uncertainty or extreme volatility;

(b) their assessment of Client suitability for relevant products or services, including but not limited to the nature, features, costs, complexity and risks of investment services, Digital Assets or other financial instruments selected for their Clients;

(c) how they ensure all Directors and Employees Managing Investments to Clients are sufficiently competent;

(d) the nature and frequency of reports to be provided to Clients; and

(e) such other policies and procedures as the AFSA may require from time to time.

(5) All Digital Asset Service Providers specified in (1) to (4) must assess and, in any case, at least yearly review the effectiveness of their policies and procedures and take appropriate measures to address any deficiencies.

### 3.5.2. Public disclosures

(1) All Digital Asset Service Providers specified in (1) to (4) in DAA 3.5.1. must publish on their website in a prominent place or make available by other publicly accessible means:

(a) a detailed description of any actual or potential conflicts of interest arising out of their activities, and how these are managed; and

(b) their policies and procedures relating to data privacy, whistleblowing and handling of Client complaints.

(2) In addition to (1), a Digital Asset Service Provider carrying out a Regulated Activity of Advising on Investments must publish on their website in a prominent place or make available by other publicly accessible means:

(a) a statement of whether the Digital Asset Service Provider refers or introduces Clients to other Persons including, but not limited to, other Digital Asset Service Providers, and if so, a description of the terms of such arrangements, and the monetary or non-monetary benefits received by the Digital Asset Service Provider, including by way of reciprocation for any service or business; and

(b) a statement of whether the Digital Asset Service Provider has accounts, funds or Digital Assets maintained by a third party and if so, provide the identity of that third party.

(3) In addition to (1), a Digital Asset Service Provider carrying out Regulated Activities of Dealing in Investments as Principal or Agent must publish on their website in a prominent place or make available by other publicly accessible means:

(a) a statement as to the Digital Asset Service Provider's arrangements for the protection of Clients' ownership of assets held by the Digital Asset Service Provider;

(b) a statement of whether the Digital Asset Service Provider refers or introduces Clients to other Persons including, but not limited to, other Digital Asset Service Providers and, if so, a description of the terms of such arrangements and the monetary or non-monetary benefits received by the Digital Asset Service Provider, including by way of reciprocation for any service or business; and

(c) a statement of whether the Digital Asset Service Provider has accounts, funds or Digital Assets maintained by a third party and if so, provide the identity of that third party.

(4) In addition to (1), a Digital Asset Service Provider carrying out a Regulated Activity of Providing Custody must publish on its website in a prominent place or make available by other publicly accessible means a statement of whether the Digital Asset Service Provider has accounts, funds or Digital Assets maintained by a third party and if so, provide the identity of that third party.

(5) In addition to (1), a Digital Asset Service Provider carrying out a Regulated Activity of Managing Investments must publish on its website in a prominent place or make available by other publicly accessible means:

(a) a statement as to the ability of Clients to have access to and withdraw their Digital Assets, particularly in times of extreme volatility;

(b) a statement as to the Digital Asset Service Provider's arrangements for the protection of Clients' assets held by the Digital Asset Service Provider;

(c) a statement as to how it protects Client Digital Assets from a counterparty risk;

(d) a statement as to how in the course of Managing Investments, Client Digital Assets are used and how Clients' interests in relation to those Digital Assets are thereby respected;

(e) a statement explaining that Client Digital Assets used by the Digital Asset Service Provider in the course of Managing Investments may be at risk, including the types and nature of such risks, and a statement on the likelihood and severity of any losses which may be suffered;

(f) a statement in relation to order execution by the Digital Asset Service Provider, which includes an explanation of how orders will be executed;

(g) a statement as to how liquidity risk is managed; and

(h) such other information as the AFSA may require from time to time.

### 3.6. Requirements for Digital Asset Service Providers Advising on Investments and Arranging Deals in Investments

**Guidance:** A Digital Asset Service Provider which carries on a Regulated Activity of Advising on Investments in relation to Digital Assets is an Authorised Firm to which provisions of the following AIFC Acts apply either directly or in respect of its officers and Employees who are Approved or Designated Individuals:

FSFR (in whole);

AML (in whole);

Chapter 2 (Client classification) of the COB;

Chapter 3 (Communication with Clients and Financial Promotions) of the COB;

Chapter 4 (Key information and client agreement) of the COB;

COB 5.2 (Suitability assessment) of the COB;

Chapter 7 (Conflicts of interest) of the COB;

Chapter 10 (Investment research) of the COB;

Chapter 15 (Complaints handling and dispute resolution) of the COB;

Chapter 16 (Record keeping and internal audit) of the COB;

Chapter 2 (Controlled and Designated Functions) of the GEN;

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN;

Chapter 6 (Supervision) of the GEN; and

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

#### 3.6.1. Verification of information

(1) In addition to requirements set out in Chapter 3 of the COB, a Digital Asset Service Provider Advising on Investments must provide advice which does not contain statements, promises, forecasts or other types of information which it knows or suspects to be misleading, false or deceptive or which it should have reasonably known to be misleading, false or deceptive at the time of making such statement, promise or forecast.

(2) Prior to making any statement, promise or forecast, a Digital Asset Service Provider Advising on Investments must verify factual information against appropriate and reliable source materials and must use all reasonable endeavours to verify the continued accuracy of such information.

### 3.6.2. Methodology

A Digital Asset Service Provider in the course of Advising on Investments must assess a broad range of Digital Assets available to the Client which should be sufficiently diverse such that the Client's investment objectives, as agreed with the Digital Asset Service Provider, are met. A Digital Asset Service Provider must be clear with Clients what range of Digital Assets have been considered in the course of Advising on Investments.

### 3.6.3. Appropriateness test

(1) A Digital Asset Service Provider Arranging Deals in Investments must not carry on a Regulated Activity with or for a Retail Client unless the Digital Asset Service Provider has carried out an appropriateness test of the Retail Client and formed a reasonable view that the Retail Client has:

(a) adequate skills and expertise to understand the risks involved in trading in Digital Assets or Digital Asset Derivatives (as the case may be); and

(b) the ability to absorb potentially significant losses resulting from trading in Digital Assets or Digital Asset Derivatives (as the case may be).

(2) A Digital Asset Service Provider must maintain records of the appropriateness test that it carries out in respect of each Retail Client and make such records available to the AFSA on request.

(3) A Digital Asset Service Provider must have appropriate systems and controls and policies and procedures to determine the appropriateness of Retail Clients

**Guidance:**

(1) To form a reasonable view referred to in DAA 3.6.3.(1) in relation to a Retail Client, a Digital Asset Service Provider should consider issues such as whether the Retail Client:

(a) has sufficient knowledge and experience relating to the type of a Digital Asset or Digital Asset Derivative offered, having regard to such factors as:

(i) how often and in what volumes that Person has traded in the relevant type of a Digital Asset or Digital Asset Derivative; and

(ii) the Retail Client's relevant qualifications, profession or former profession;

(b) understands the characteristics and risks relating to Digital Assets or Digital Asset Derivatives, and the volatility of their prices;

(c) understands the impact of leverage, due to which, there is potential to make significant losses in trading in Digital Assets or Digital Asset Derivatives; and

(d) has the ability, particularly in terms of net assets and liquidity available to the Retail Client, to absorb and manage any losses that may result from trading in the Digital Assets or Digital Asset Derivatives offered.

(2) To be able to demonstrate to the AFSA that it complies with DAA 3.6.3., a Digital Asset Service Provider should have in place systems and controls that include:

(a) pre-determined and clear criteria against which a Retail Client's ability to trade in Digital Assets or Digital Asset Derivatives can be assessed;

(b) adequate records to demonstrate that the Digital Asset Service Provider has undertaken the appropriateness test for each Retail Client; and

(c) in the case of an existing Retail Client with whom the Digital Asset Service Provider has previously traded in Digital Assets or Digital Asset Derivatives, procedures to undertake a fresh appropriateness test on at least an annual basis, and if:

(i) a new Digital Asset or Digital Asset Derivative with a materially different risk profile is offered to the Retail Client; or

(ii) there has been a material change in the Retail Client's circumstances.

(3) If a Digital Asset Service Provider forms the view that it is not appropriate for a Person to trade in Digital Assets or Digital Asset Derivatives, the Digital Asset Service Provider should refrain from offering that service to the Person. As a matter of good practice, the Digital Asset Service Provider should inform the Person of its decision.

### 3.7. Requirements for Digital Asset Service Providers Providing and Arranging Custody

**Guidance:** A Digital Asset Service Provider which carries on a Regulated Activity of Providing Custody in relation to Digital Assets is an Authorised Firm to which provisions of the following AIFC Acts apply either directly or in respect of its officers and Employees who are Approved or Designated Individuals:

FSFR (in whole);

AML (in whole);

Chapter 2 (Client classification) of the COB;

Chapter 3 (Communication with Clients and Financial Promotions) of the COB;

Chapter 4 (Key information and client agreement) of the COB;

Chapter 7 (Conflicts of interest) of the COB;

Chapter 8 (Client Assets) of the COB;

Chapter 15 (Complaints handling and dispute resolution) of the COB;

Chapter 16 (Record keeping and internal audit) of the COB;

Chapter 2 (Controlled and Designated Functions) of the GEN;

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN;

Chapter 6 (Supervision) of the GEN; and

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

A Digital Asset Service Provider which carries on a Regulated Activity of Arranging Custody in relation to Digital Assets is an Authorised Firm to which provisions of the following AIFC Acts apply either directly or in respect of its officers and Employees who are Approved or Designated Individuals:

AML (in whole);

Chapter 2 (Client classification) of the COB;

COB 8.3.7 (on assessing the suitability of Third Party Account Providers);

COB 8.3.13 (on disclosure);

COB 8.3.14(2) (on client reporting);

COB 8.3.15 (on record keeping);

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN; and

Chapter 6 (Supervision) of the GEN.

### 3.7.1. Requirements for Digital Asset Service Providers Providing Custody of Digital Assets

(1) A Digital wallet Service Provider must ensure that:

(a) they are recorded, registered and held in an appropriate manner to safeguard and control them, including the fact that they must be held separately from the Digital Asset Service Provider's own Digital Assets.

(b) any DLT application it uses in Providing Custody of Digital Assets is resilient, reliable and compatible with any relevant facility on which the Digital Assets are traded or cleared;

(c) it has in place Client agreements which specify the basis on which it holds Digital Assets on behalf of its Clients, and in particular whether they are held:

(i) on a segregated basis, in which case the Digital Asset Service Provider which is a Digital wallet Service Provider needs to clearly identify and segregate Digital Assets belonging to different Clients; or

(ii) on an omnibus basis, in which case the Digital Asset Service Provider which is a Digital wallet Service Provider needs to ensure at all times that the total amount and type of Digital Assets held for Clients at all times matches the amounts it has agreed to hold for all its Clients, and that there are clear records regarding the amount of Digital Assets held for each Client; and

(d) it has in place appropriate procedures to enable it to confirm Client instructions and transactions, maintain appropriate records and data relating to those instructions and transactions and to conduct a reconciliation of those transactions at appropriate intervals.

(2) A Digital wallet Service Provider must ensure that, in developing and using DLT applications and other technology to Provide Custody of Digital Assets:

(a) the architecture of any Digital wallet used adequately addresses potential compatibility issues and associated risks;

(b) the technology used and its associated procedures have adequate security measures (including enabling adequate cyber security) to enable the safe storage and transmission of data relating to the Digital Assets;

(c) the security and integrity of cryptographic keys are maintained through the use of that technology, taking into account the password protection and methods of encryption used;

(d) there are adequate measures to address any risks specific to the methods of usage and storage of cryptographic keys (or their equivalent) available under the DLT application used; and

(e) the technology is compatible with the procedures and protocols built into the relevant rules or equivalent procedures and protocols on any facility on which the Digital Assets are traded or cleared or both traded and cleared.

(3) Digital Assets held by the Digital Asset Service Provider Providing Custody are not depository liabilities or assets of the Digital Asset Service Provider and the Digital Asset Service Provider must hold them on trust.

(4) A Digital Asset Service Provider Providing Custody of Digital Assets must segregate the Digital Assets of each Client in separate Digital wallets containing the Digital Assets of that Client only.

(5) A Digital Asset Service Provider Providing Custody must maintain control of each Digital Asset at all times while Providing Custody.

(6) A Digital Asset Service Provider Providing Custody must:

(a) have appropriate rules, procedures, and controls, including robust accounting practices, to safeguard the rights of Digital Assets issuers and holders, prevent the unauthorised creation or deletion of Digital Assets, and conduct daily reconciliation of each Digital Asset balance it maintains for issuers and holders;

(b) prohibit overdrafts and credit balances in Digital Assets account;

(c) maintain Digital Assets in an immobilised or dematerialised form for their transfer by book entry;

(d) protect assets against custody risk through appropriate rules and procedures consistent with its legal framework;

(e) ensure segregation between its own assets and the Digital Assets of its participants, as well as keeping clear records regarding which Digital Assets belong to which participant; and

(f) identify, measure, monitor, and manage its risks from other activities that it may perform.

**Guidance:**

Where an Authorised Person which is a Digital wallet Service Provider delegates any functions to a Third Party Digital wallet Service provider, it must ensure that the delegate fully complies with the requirements of DAA 3.7.1. and the outsourcing and delegation requirements of GEN 5.2.

Delegation of any functions to a Third Party Digital wallet Service provider must not affect a Digital wallet Service Provider's responsibility for the full and proper performance of those functions.

### 3.7.2. Digital wallet management

(1) Requirements in relation to Hot and Cold Digital wallet storage.

(a) A Digital wallet Service Provider must at all times maintain appropriate certifications as may be required under industry best practices applicable to the safekeeping of Digital Assets.

(b) Where a Digital wallet Service Provider uses a variety of storage mechanisms for Digital Assets, the Digital wallet Service Provider should conduct a risk-based analysis to determine the appropriate method of Digital Asset storage for different Digital Assets.

(c) Where a Digital wallet Service Provider uses a single storage mechanism for Digital Assets, the Digital wallet Service Provider should explicitly disclose to Clients any limitations regarding the suitability of that storage mechanism for different Digital Assets.

(d) A Digital wallet Service Provider should document in detail the methodology for determining when Digital Assets are transferred to and from Digital wallets. The mechanisms for transfer between different types of Digital wallets should be well documented and subject to internal controls and audits performed by an independent third-party auditor.

(2) Seed or key generation, storage, and use.

(a) To ensure a secure generation mechanism, a Digital wallet Service Provider must use industry best standards to create the seed, including by using asymmetric private and public key combinations, or other similar mechanisms.

(b) A Digital wallet Service Provider must consider all risks associated with producing a private key or seed for a signatory including whether the signatory should be involved in the generation process or whether creators of the seed, private key, or other similar mechanism should be prohibited from cryptographically signing any transaction or from having access to any relevant systems.

(c) A Digital wallet Service Provider must adopt industry best practices when using encryption and secure device storage for a Client's private keys when not in use.

(d) A Digital wallet Service Provider must ensure that any keys stored online or in one physical location are not capable of being used to conduct a Digital Asset transaction, unless appropriate controls are in place to ensure that access by an unauthorised individual is insufficient to conduct a transaction.

(e) All key and seed backups must be stored in a separate location from the primary key and seed. Key and seed backups must be stored with encryption at least equal to the encryption used to protect the primary seed and key.

(f) Digital wallet Service Providers must mitigate the risk of collusion between all authorised parties or signatories who are able to authorise the movement, transfer or withdrawal of Digital Assets held on behalf of Clients. The risk of collusion and other internal points of failure should be addressed during recurring operational risk assessments.

(3) Lost or stolen keys.

(a) Digital wallet Service Providers must establish and maintain effective policies and procedures in the event that any seed or cryptographic keys of any Digital wallet are lost or otherwise compromised.

(b) The policy and procedures must address matters including but not limited to:

(i) recovery of affected Digital Assets;

(ii) timely communications with all Clients and counterparties regarding consequences arising from relevant incidents and measures being taken to remedy such consequences;

(iii) cooperation with law enforcement agencies and regulatory bodies; and

(iv) if applicable, preparation of winding down arrangements and public disclosure of such arrangements.

### 3.7.3. Contractual arrangement

A Digital Asset Service Provider that is Providing Custody for a Client should provide such activity based on a contractual arrangement. Under such an arrangement a Client is lawfully in control of, or entitled to control, a Digital Asset. Transfers of control of the Digital Asset to a Digital Asset Service Provider solely for the purpose of receiving custody services does not in any way transfer to the Digital Asset Service Provider any legal interest in the Digital Asset or any discretionary authority not stated in the Client Agreement or otherwise agreed to by the Client.

### 3.7.4. Client Agreement for a Digital Asset Service Provider Providing Custody of Digital Assets

A Digital Asset Service Provider Providing Custody of Digital Assets must enter into a Client Agreement with each Client that includes:

(a) a breakdown of all fees and charges payable to or via the Digital Asset Service Provider and when they are charged;

(b) any information required to carry out a transfer;

(c) the form and procedures for giving consent to a transfer;

(d) an indication of the time it will normally take to carry out a transfer;

(e) details of when a transfer will be considered to be complete;

(f) how, and in what form, information and communications relating to transfer services will be provided to the Client, including the timing and frequency of communications, the language used and any technical requirements for the Client's equipment and software to receive the communications;

(g) clear policies and procedures relating to unauthorised or incorrectly executed transfers, including the circumstances in which the Client is and is not entitled to redress;

(h) clear policies and procedures relating to how situations where the holding or transfer of Digital Assets may have been compromised are dealt with, such as if there has been hacking, theft or fraud;

(i) details of the procedures the Authorised Firm will follow to contact the Client, or which the Client may use to contact the Authorised Firm if there has been suspected or actual hacking, theft or fraud; and

(j) the mechanisms by which the Client can keep track of Digital Assets held with the Digital Asset Service Provider.

### 3.7.5. Client accounts

(1) A Digital Asset Service Provider which Provides Custody or holds or controls Client Digital Assets must register or record all Digital Assets in the legal title of a Client Account or, where this is not feasible, for example, due a legal requirement or market practice, the Digital Asset Service Provider.

(2) A Client Account is an account which:

(a) is held with a Third Party Agent or by a Digital Asset Service Provider which is authorised under its Licence to carry on the Regulated Activity of Providing Custody;

(b) is established to hold Client Digital Assets;

(c) when held by a Third Party Agent, is maintained in the name of;

(i) if a Domestic Firm, the Digital Asset Service Provider; or

(ii) if not a Domestic Firm, a Nominee Company controlled by the Digital Asset Service Provider; and

(d) includes the words 'Client Account' in its title.

(3) A Digital Asset Service Provider must maintain a master list of all Client Accounts for 6 years from the closure of the relevant acount that must detail:

(a) the name of the account;

(b) the account number;

(c) the location of the account;

(d) whether the account is currently open or closed; and

(e) the date of opening or closure.

(4) A Digital Asset Service Provider which intends to use the Client's Digital Assets for its own purpose or that of another Person, must have systems and controls in place to ensure that:

(a) it obtains that Client's prior explicit informed written consent to such use, and that Clients are aware of the risks incurred in giving such consent;

(b) adequate records are maintained to record how Digital Assets are applied as collateral or used for stock lending activities;

(c) equivalent assets are returned to the Client Account of the Client; and

(d) the Client is not disadvantaged by such use of his Digital Assets in any way in which the Client has not explicitly consented to.

### 3.7.6. Client disclosure

(1) Before a Digital Asset Service Provider arranges custody for a Client it must disclose to that Client, if applicable, that the Client's Digital Assets may be held in a jurisdiction outside the AIFC and that the market practices, insolvency and legal regime applicable in that jurisdiction may differ from the regime applicable in the AIFC.

(2) Before a Digital Asset Service Provider provides custody for a Client it must disclose to the Client on whose behalf the Digital Assets will be held:

(a) the arrangements for recording and registering Digital Assets, claiming and receiving any entitlements, and the giving and receiving instructions relating to them;

(b) the obligations the Digital Asset Service Provider will have to the Client in relation to exercising rights on behalf of the Client;

(c) the basis on which, and any terms governing the way in which, Digital Assets will be held, including any rights which the Digital Asset Service Provider may have to realise Digital Assets held on behalf of the Client in satisfaction of a default by the Client;

(d) the method and frequency with which the Digital Asset Service Provider will report to the Client in relation to his Digital Assets;

(e) if applicable, a statement that the Digital Asset Service Provider intends to pool Digital Assets with those of other Clients;

(f) if applicable, a statement that the Client's Digital Assets may be held in a jurisdiction outside the AIFC and the market practices, insolvency and legal regime applicable in that jurisdiction may differ from the regime applicable in the AIFC;

(g) if applicable, a statement that the Digital Asset Service Provider holds or intends to hold Digital Assets in a Client Account with a Third Party Agent which is in the same Group as the Digital Asset Service Provider; and

(h) the extent of the Digital Asset Service Provider's liability in the event of default by a Third Party Agent, and any rights that the Client may have in respect of the Third Party Agent.

### 3.7.7. Client reporting

(1) A Digital Asset Service Provider which provides custody or which holds or controls Digital Assets for a Client must send a statement to each Client at least every 6 months.

(2) The statement must include:

(a) a list of that Client's Digital Assets as at the date of reporting;

(b) a list of that Client's Collateral and the market value of that Collateral as at the date of reporting; and

(c) details of any Client Money held by the Digital Asset Service Provider as at the date of reporting.

(3) The statement must be sent to the Client within 25 business days of the statement date.

### 3.7.8. Reconciliation

(1) A Digital Asset Service Provider which carries out a Regulated Activity of Providing Custody or Arranging Custody must:

(a) (where the Digital Asset Service Provider is Arranging Custody) at least every 25 business days reconcile its records of Client Accounts held with Third Party Agents with monthly statements received from those Third Party Agents in respect of each individual Client's ledger balances; or

(b) (where the Digital Asset Service Provider is Providing Custody) at least every 25 business days perform an internal custody record reconciliation in respect of each individual Client's ledger balances.

(2) A Digital Asset Service Provider must ensure that the process of reconciliation does not involve any conflict of interest in terms of providing a full and accurate reconciliation.

### 3.7.9. Requirements where shortfalls or discrepancies are detected

(1) Where a Digital Asset Service Provider identifies a discrepancy as a result of carrying out an internal record check or an external custody reconciliation, the Digital Asset Service Provider must:

(a) promptly take all reasonable steps to investigate and resolve the discrepancy;

(b) take appropriate steps for the treatment of any shortfalls until the discrepancy is resolved;

(c) take reasonable steps to avoid a recurrence of any identifiable action which resulted in the discrepancy; and

(d) notify the AFSA where the discrepancy is material or otherwise cannot be promptly resolved.

(2) A discrepancy should not be considered resolved until it is investigated fully and corrected, and any associated shortfall is resolved by the Digital Asset Service Provider ensuring that:

(a) it is holding the correct Digital Assets for each of its Clients; and

(b) its own records, and the records of any relevant Third Party Digital wallet Service Provider, are accurate.

(3) Where a shortfall is detected, until such a shortfall is resolved, the Digital Asset Service Provider must do one of the following:

(a) allocate a specific number of its own applicable Digital Assets to cover the value of the shortfall and hold them in such a way for the relevant Clients so that the proceeds of their liquidation will be available for the benefit of the relevant Clients in the event of the Digital Asset Service Provider's failure; or

(b) appropriate a sufficient amount of its own money to cover the value of the shortfall and hold it for the relevant Client(s).

(4) The value of any shortfall must be determined by reference to the previous day's closing mark to market valuation of the relevant Digital Assets, or, if that information is not available in relation to a particular Digital Asset, the most recently available valuation information. If the value of a Digital Asset is volatile or there are any other reasons which make it difficult to value, the Digital Asset Service Provider should consider whether it is appropriate to set aside an additional amount to cover any change in the value of the shortfall.

(5) Until the discrepancy is resolved the Digital Asset Service Provider must consider whether it would be appropriate to notify affected Client(s) of the situation. In considering whether to notify Clients, the Digital Asset Service Provider must act honestly, fairly and professionally and in the best interests of its Client(s).

**Guidance**

(1) A Digital Asset Service Provider should maintain a clear separation of duties to ensure that all Employees with responsibility for operating Client Accounts, or who have authority over Digital Assets held for Clients, should not perform the reconciliations under DAA 3.7.8.

(2) Reconciliations performed in accordance with DAA 3.7.8. must be reviewed by a member of the Digital Asset Service Provider who is a member of the Board.

(3) The individual referred to in (2) must provide a written statement confirming that the reconciliation has been undertaken in accordance with the requirements of DAA 3.7.8 and this Guidance.

(4) A material discrepancy includes discrepancies which have the cumulative effect of being material, such as longstanding discrepancies.

## 3.8. Requirements for Digital Asset Service Providers Managing Investments and a Collective Investment Scheme

**Guidance:** A Digital Asset Service Provider which carries on a Regulated Activity of Managing Investments in relation to Digital Assets is an Authorised Firm to which provisions of the following AIFC Acts apply either directly or in respect of its officers and Employees who are Approved or Designated Individuals:

FSFR (in whole);

AML (in whole);

Chapter 2 (Client classification) of the COB;

Chapter 3 (Communication with Clients and Financial Promotions) of the COB;

Chapter 4 (Key information and client agreement) of the COB;

COB 5.2 (Suitability assessment);

Chapter 7 (Conflicts of interest) of the COB;

Chapter 15 (Complaints handling and dispute resolution) of the COB;

Chapter 16 (Record keeping and internal audit) of the COB;

Chapter 2 (Controlled and Designated Functions) of the GEN;

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN;

Chapter 6 (Supervision) of the GEN; and

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

A Digital Asset Service Provider which carries on a Regulated Activity of Managing a Collective Investment Scheme in relation to Digital Assets is an Authorised Firm to which provisions of the following AIFC Acts apply either directly or in respect of its officers and Employees who are Approved or Designated Individuals:

FSFR (in whole);

AML (in whole);

Chapter 2 (Client classification) of the COB;

Chapter 3 (Communication with Clients and Financial Promotions) of the COB;

Chapter 4 (Key information and client agreement) of the COB;

Chapter 7 (Conflicts of interest) of the COB;

Chapter 15 (Complaints handling and dispute resolution) of the COB;

Chapter 16 (Record keeping and internal audit) of the COB;

Chapter 2 (Controlled and Designated Functions) of the GEN;

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN;

Chapter 6 (Supervision) of the GEN; and

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

### 3.8.1. Verification of information

(1) In addition to requirements set out in Chapter 3 of the COB, a Digital Asset Service Provider Managing Investments or a Collective Investment Scheme must not provide statements, promises, forecasts or other types of information which it knows or suspects to be misleading, false or deceptive or which it should have reasonably known to be misleading, false or deceptive at the time of making such statement, promise or forecast.

(2) Prior to making any statement, promise or forecast, a Digital Asset Service Provider Managing Investments or a Collective Investment Scheme must verify factual information against appropriate and reliable source materials and must use all reasonable endeavours to verify the continued accuracy of such information (for as long as such information is communicated by or on behalf of the Digital Asset Service Provider). A Digital Asset Service Provider should state the date on which the information was last verified in the relevant communication.

### 3.8.2. Client reporting and valuation

(1) A Digital Asset Service Provider Managing Investments or a Collective Investment Scheme must, at least monthly, provide to each of its Clients a written statement containing the following information:

(a) the total value of Digital Assets in a Client's account; and

(b) the change in amount and valuation of Digital Assets in a Client's account during the relevant reporting period.

(2) A Digital Asset Service Provider Managing Investments or a Collective Investment Scheme must ensure that all assets under management are subject to ongoing independent valuation.

(3) A Digital Asset Service Provider Managing Investments or a Collective Investment Scheme must have comprehensive and well documented valuation policies and procedures in place to ensure the production of timely and accurate statement in accordance with DAA 3.8.2. (1).

### 3.8.3. Risk management and due diligence

(1) A Digital Asset Service Provider Managing Investments or a Collective Investment Scheme must ensure that liquidity risk and market risk are each monitored and tested regularly, and appropriate measures are in place as required to address any such risk in a prompt manner.

(2) All such risk management and due diligence must be audited by an independent third party on an annual basis and provided to the AFSA upon request.

### 3.8.4. Content of confirmation notes

For the purposes of COB 9.1.3., a Digital Asset Service Provider Managing a Collective Investment Scheme must include the following general information:

(a) the Digital Asset Service Provider's name and address;

(b) a description of the Digital Assets;

(c) whether the Transaction is a sale or purchase;

(d) the price or unit price at which the Transaction was executed;

(e) if applicable, a statement that the Transaction was executed on an execution-only basis;

(f) the date and time of the Transaction;

(g) the amount the Digital Asset Service Provider charges in connection with the Transaction, including Commission charges and the amount of any Mark-up or Mark-down, Fees, taxes or duties;

(h) the amount or basis of any amounts received from another Person in connection with the services; and

(i) a statement that the price at which the Transaction has been Executed is on a Historic Price or Forward Price basis, as the case may be.

(2) A Digital Asset Service Provider may combine items (f) and (j) above in respect of a Transaction where the Client has requested a note showing a single price combining both of these items.

## 3.9. Requirements for Digital Asset Service Providers Dealing in Investments as Principal or Agent

**Guidance:** A Digital Asset Service Provider which carries on a Regulated Activity of Dealing in Investments as Principal or Agent in relation to Digital Assets is an Authorised Firm to which provisions of the following AIFC Acts apply either directly or in respect of its officers and Employees who are Approved or Designated Individuals:

FSFR (in whole);

AML (in whole);

Chapter 2 (Client classification) of the COB;

Chapter 3 (Communication with Clients and Financial Promotions) of the COB;

Chapter 4 (Key information and client agreement) of the COB;

COB 5.3 (Appropriateness assessment);

Chapter 6 (Order execution and order handling) of the COB;

Chapter 7 (Conflicts of interest) of the COB;

Chapter 9 (Reporting to Clients) of the COB;

Chapter 15 (Complaints handling and dispute resolution) of the COB;

Chapter 16 (Record keeping and internal audit) of the COB;

Chapter 2 (Controlled and Designated Functions) of the GEN;

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN;

Chapter 6 (Supervision) of the GEN; and

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC (in whole).

### 3.9.1. Content of confirmation notes

For the purposes of COB 9.1.3., a Digital Asset Service Provider must include the following general information:

(a) the Digital Asset Service Provider's name and address;

(b) whether the Digital Asset Service Provider executed the Transaction as principal or agent;

(c) a description of the Digital Asset;

(d) whether the Transaction is a sale or purchase;

(e) the price or unit price at which the Transaction was executed;

(f) if applicable, a statement that the Transaction was executed on an execution-only basis;

(g) the date and time of the Transaction;

(h) the total amount payable by the Client and the date on which it is due;

(i) the amount the Digital Asset Service Provider charges in connection with the Transaction, including Commission charges and the amount of any Mark-up or Mark-down, Fees, taxes or duties; and

(j) the amount or basis of any amounts received from another Person in connection with the services.

(2) A Digital Asset Service Provider may combine items (f) and (j) above in respect of a Transaction where the Client has requested a note showing a single price combining both of these items.

### 3.9.2. Appropriateness test

(1) A Digital Asset Service Provider Dealing in Investments as Principal or Agent must not carry on a Regulated Activity with or for a Retail Client unless the Digital Asset Service Provider has carried out an appropriateness test of the Retail Client and formed a reasonable view that the Retail Client has:

(a) adequate skills and expertise to understand the risks involved in trading in Digital Assets or Digital Asset Derivatives (as the case may be); and

(b) the ability to absorb potentially significant losses resulting from trading in Digital Assets or Digital Asset Derivatives (as the case may be).

(2) A Digital Asset Service Provider must maintain records of the appropriateness test that it carries out in respect of each Retail Client and make such records available to the AFSA on request.

(3) A Digital Asset Service Provider must have appropriate systems and controls and policies and procedures to determine the appropriateness of Retail Clients.

**Guidance:**

(1) To form a reasonable view referred to in DAA 3.9.2.(1) in relation to a Retail Client, a Digital Asset Service Provider should consider issues such as whether the Retail Client:

(a) has sufficient knowledge and experience relating to the type of a Digital Asset or Digital Asset Derivative offered, having regard to such factors as:

(i) how often and in what volumes that Person has traded in the relevant type of a Digital Asset or Digital Asset Derivative; and

(ii) the Retail Client's relevant qualifications, profession or former profession;

(b) understands the characteristics and risks relating to Digital Assets or Digital Asset Derivatives, and the volatility of their prices;

(c) understands the impact of leverage, due to which, there is potential to make significant losses in trading in Digital Assets or Digital Asset Derivatives; and

(d) has the ability, particularly in terms of net assets and liquidity available to the Retail Client, to absorb and manage any losses that may result from trading in the Digital Assets or Digital Asset Derivatives offered.

(2) To be able to demonstrate to the AFSA that it complies with DAA 3.9.2., a Digital Asset Service Provider should have in place systems and controls that include:

(a) pre-determined and clear criteria against which a Retail Client's ability to trade in Digital Assets or Digital Asset Derivatives can be assessed;

(b) adequate records to demonstrate that the Digital Asset Service Provider has undertaken the appropriateness test for each Retail Client; and

(c) in the case of an existing Retail Client with whom the Digital Asset Service Provider has previously traded in Digital Assets or Digital Asset Derivatives, procedures to undertake a fresh appropriateness test on at least an annual basis, and if:

(i) a new Digital Asset or Digital Asset Derivative with a materially different risk profile is offered to the Retail Client; or

(ii) there has been a material change in the Retail Client's circumstances.

(3) If a Digital Asset Service Provider forms the view that it is not appropriate for a Person to trade in Digital Assets or Digital Asset Derivatives, the Digital Asset Service Provider should refrain from offering that service to the Person. As a matter of good practice, the Digital Asset Service Provider should inform the Person of its decision.

### 3.10. Provision of key features document and disclosure of risks

#### 3.10.1. Provision of key features document to Person

(1) A Digital Asset Service Provider which carries on any one or more of the following Regulated Activities in relation to Digital Assets:

(a) Dealing in Investments as Principal;

(b) Dealing in Investments as Agent;

(c) Advising on Investments; and

(d) Arranging Deals in Investments,

must not provide that service or services to a Person unless it has provided the Person with a key features document.

(2) The key features document must contain the following information if known (or, if not known after having taken reasonable steps to determine this information, a clear statement must be provided that such information is not known):

(a) risks associated with and essential characteristics of the Digital Assets, including where appropriate making reference to the location of any publicly available white paper setting out the features of the Digital Assets;

(b) risks associated with and essential characteristics of the Digital Asset;

(c) whether the Digital Asset is admitted to trading within the AIFC;

(d) (where the Digital Asset Service Provider is involved in Providing Custody or Arranging Custody of the Digital Asset) whether the Client, the Digital Asset Service Provider or a third party is responsible for providing a Digital wallet service in respect of the Digital Asset, and any related risks (including at whose risk the Client's Digital Assets are held in the Digital wallet, whether it is accessible online or stored offline, what happens if keys to the Digital wallet are lost and what procedures can be followed in such an event);

(e) how the Client may exercise any rights conferred by the Digital Assets; and

(f) any other information relevant to the particular Digital Asset which would reasonably assist the Client to to make informed decisions in respect of it.

(3) The key features document must be provided in good time before the relevant service is provided to a Client, so that the Client to make an informed decision about whether to use the relevant service.

(4) The key features document does not need to be provided to a Client to whom the Digital Asset Service Provider has previously provided that information, if there has been no significant change since the information was previously provided.

(5) A Digital Asset Service Provider may use a key features document prepared by another Person if it has taken reasonable steps to ensure that the information in that document is complete, accurate and up to date.

(6) If a Digital Asset Service Provider provides a Client with a key features document prepared by another Person, the Digital Asset Service Provider remains accountable to the Client to whom the key features document is provided as if that document were prepared by the Digital Asset Service Provider itself.

### 3.10.2. Risk warnings

(1) A Digital Asset Service Provider must display prominently on its website the following risk warnings relating to Digital Assets:

(a) (except in the case of a Central Bank Digital Currency) that Digital Assets are not legal tender or backed by a government;

(b) that Digital Assets are subject to extreme volatility and the value of the Digital Asset can fall quickly (including, in respect of a Fiat stablecoin or Commodity stablecoin, if it loses its stability peg);

(c) that an investor in Digital Assets may lose all, or part, of the value of their investment;

(d) that Digital Assets may not always be liquid or transferable;

(e) that investments in Digital Assets may be complex making it hard to understand the risks associated with participating in them;

(f) that Digital Assets can be stolen because of cyber attacks;

(g) that trading in Digital Assets is susceptible to irrational market forces;

(h) that the nature of Digital Assets may lead to an increased risk of Financial Crime;

(i) there being limited or, in some cases, no mechanisms for the recovery of lost or stolen Digital Assets;

(j) the risks of Digital Assets with regard to anonymity, irreversibility of transactions, accidental transactions, transaction recording, and settlement;

(k) that the nature of Digital Assets means that technological difficulties experienced by a Digital Asset Trading Facility Operator may prevent access to or use of a Client's Digital Assets;

(l) that participating in Digital Assets is not comparable to participating in traditional investments such as Securities; and

(m) that there is no recognised compensation scheme to provide an avenue of redress for aggrieved participants.

(2) If a Digital Asset Service Provider presents any marketing or educational materials and other communications relating to a Digital Asset on a website, in the general media or as part of a distribution made to existing or potential new Clients, it must include the risk warning referred to in 3.10.2 (1) in a prominent place at or near the top of each page of the materials or communication.

(3) If the material referred to in 3.10.2 (1) is provided on a website or an application that can be downloaded to a mobile device, the warning must be:

(a) statically fixed and visible at the top of the screen even when a person scrolls up or down the webpage;

(b) included on each linked webpage on the website; and

(c) If, due to limitations on the medium of communication used, it is not practicable to provide the material referred to in DAA 2.8.10(1), reference may be made instead to the fact that participation in Digital Assets is a high risk investment, accompanied with a link to the relevant section of the Digital Asset Service Provider's website where the material referred to in DAA 2.8.10 (1) is provided.

### 3.10.3. Past performance and forecasts of Digital Assets

(1) A Digital Asset Service Provider must ensure that any information or representation relating to past performance, or any future forecast based on past performance or other assumptions, which is provided to or targeted at Retail Clients:

(a) presents a fair and balanced view of the Digital Assets and associated services to which the information or representation relates;

(b) identifies, in an easy-to-understand manner, the source of information from which the past performance is derived and any key facts and assumptions used in that context are clearly explained; and

(c) contains a clear and prominent warning that past performance is not necessarily a reliable indicator of future results.

(2) A Digital Asset Service Provider should in providing information about the past performance of a Digital Asset:

(a) consider the knowledge and sophistication of the audience to whom the information is targeted;

(b) fully disclose the source and the nature of the past performance presented;

(c) ensure that the time period used is not an inappropriately short period, or a selective period, that is potentially misleading; and

(d) if a comparison is being made, the comparison is fair, clear and not misleading.

## 3.11. Clients

### 3.11.1. Investment limits

A Digital Asset Service Provider must maintain effective systems and controls to ensure its compliance with the requirements and limits imposed by the Rules on Currency Regulation and

Provision of Information on Currency Transactions in the AIFC when dealing with a Retail Client who is a resident of the Republic of Kazakhstan.

### 3.11.2. Calculation of an individual Client's net assets

(1) For the purposes of calculating an individual Client's net assets to treat him as an Assessed Professional Client under Rule 2.5.1(a) of the COB, the Digital Asset Service Provider:

(a) must exclude the value of the primary residence of the Client;

(b) must exclude Digital Assets belonging to the Client that are not admitted to trading;

(c) must include only 30% of the market value of a Digital Asset admitted to trading, which belongs to the Client, but must include 100% of the market value of Fiat and Commodity stablecoins backed by reserves, which belong to the Client; and

(d) may include any other assets held directly or indirectly by that Client.

## 3.12. Prohibitions

(1) A Representative Office must not market a Digital Asset or a Financial Service related to a Digital Asset.

(2) An Authorised Crowdfunding Platform Operating an Investment Crowdfunding Platform must not facilitate a Person investing in the Digital Assets.

(3) An Authorised Firm may not carry on an activity related to a Utility Token or Non-Fungible Token.

(4) The prohibition in (3) does not apply to a Digital Asset Service Provider:

(a) which is authorised to Provide Custody; and

(b) to the extent that it Provides Custody in relation to a Utility Token or Non-fungible Token.

## 3.13. Obligations

### 3.13.1. Obligation to report to the AFSA

(1) A Digital Asset Service Provider must submit to the AFSA a quarterly report that should include its financial statement, its income statement, a calculation of its relevant capital resources and a statement of its compliance and any non-compliance with these Rules.

(2) A Digital Asset Service Provider must provide the following information to the AFSA within 6 months after financial year end:

(a) the number of prospective clients which the Digital Asset Service Provider rejected during the reporting period;

(b) the number of Clients which were offboarded during the reporting period;

(c) the number of Clients where enhanced due diligence was applied;

(d) the total number of the Digital Asset Service Provider's Clients;

(e) the number of Clients originating from a high risk jurisdiction;

(f) the number of Clients on-boarded on a face-to-face basis;

(g) a description of any changes to the Client onboarding process;

(h) the number of suspicious transaction reports filed during the reporting period;

(i) the number of individuals supporting the MLRO;

(j) when the Digital Asset Service Provider's risk assessment was last updated and if there were any additional risks;

(j) (if applicable) the number of private keys held;

(k) (if applicable) whether Client's Digital Assets are held with a third party custodian;

(l)whether the Digital Asset Service Provider forms part of a group, and if so, the group structure;

(m) whether the Digital Asset Service Provider entered into any resource sharing agreements and, if so, the names of the counterparty/company;

(n)whether the Digital Asset Service Provider outsources any of its functions and, if so, any changes to the functions outsourced and to which companies;

(o) an overview of any involvement of the Digital Asset Service Provider's shareholders in the day-to-day operations of the Digital Asset Service Provider during the reporting period; and

(p) an overview of any instances of market abuse encountered by the Digital Asset Service Provider during the reporting period.

(3) The AFSA may request a Digital Asset Service Provider to submit other returns. The AFSA from time to time may prescribe the required list of returns to be submitted and the returns templates to be used.

(4) Returns submitted to the AFSA must be signed by two (2) Approved Individuals and one of them must be approved to exercise the Finance Officer function.

### 3.13.2. Obligation to notify the AFSA

If a Digital Asset Service Provider becomes aware, or has a reasonable ground to believe, that it is or may be (or may be about to be) in breach of any of these Rules it must:

(a) notify the AFSA in writing about the breach and the relevant circumstances immediately and not later than within 1 business day of becoming aware of it; and

(b) not make any cash transfers or payments or transfers of liquid assets to its Affiliates or Related Persons, whether by way of dividends or otherwise, without the AFSA's written consent.

**Guidance:**

In dealing with a breach, or possible breach, of this part, the AFSA's primary concern will be the interests of existing and prospective Clients, the potential adverse impact on market

participants, and market stability. The AFSA recognises that there will be circumstances in which a problem may be resolved quickly, for example, by support from a parent entity, without jeopardising the interests of Clients and other stakeholders. In such circumstances, it will be in the interests of all parties to minimise the disruption to the firm's business. The AFSA's will normally seek to work cooperatively with the Digital Asset Service Provider in stressed situations to deal with any problems. There will, however, be circumstances in which it is necessary to take regulatory action to avoid exposing market participants, Clients and other stakeholders to the potential adverse consequences of the Digital Asset Service Provider's Failure, and the AFSA will not hesitate to take appropriate action if it considers this necessary.

### 3.14. AFSA power to impose requirements

Without limiting the powers available to the AFSA under Part 8 of the Framework Regulations, the AFSA may direct a Digital Asset Service Provider to do or not do specified things that the AFSA considers are necessary or desirable or to ensure the integrity of the AIFC financial markets, including but not limited to directions imposing on a Digital Asset Service Provider any additional requirements that the AFSA considers appropriate.

## 4. RULES APPLICABLE TO AUTHORISED FIRMS PROVIDING MONEY SERVICES IN RELATION TO DIGITAL ASSETS AND ISSUANCE OF FIAT STABLECOINS AND COMMODITY STABLECOINS

This Part 4 applies to a Digital Asset Service Provider which is an Authorised Person carrying on, in or from the AIFC, the activities of Providing Money Services in relation to Digital Assets, issuing Fiat stablecoins and Commodity stablecoins.

**Guidance**

An Authorised Firm Providing Money Services is a Centre Participant to which provisions of the following regulations and rules apply either directly or in respect of its officers and Employees who are Approved Individuals or Designated Individuals:

FSFR (in whole);

AML (in whole);

Chapter 3 (Communications with Clients and Financial Promotions) of the COB;

Chapter 4 (Key information and client agreement) of the COB;

Chapter 7 (Conflicts of interest) of the COB;

Chapter 8 (Client Assets) of the COB;

Chapter 15 (Complaints handling and dispute resolution) of the COB;

Chapter 2 (Controlled and Designated Functions) of the GEN;

Chapter 3 (Control of Authorised Persons) of the GEN;

Chapter 4 (Core Principles) of the GEN;

Chapter 5 (Systems and Controls) of the GEN;

Chapter 6 (Supervision) of the GEN; and

Rules on Currency Regulation and Provision of Information on Currency Transactions in the AIFC.

PMS, except for PMS 3.1. (Systems and controls), PMS 3.2. (Technology governance and risk management framework), 3.4. (Cyber-security policy).

### 4.1. Authorisation

(1) A Person wishing to carry on Providing Money Services in relation to Digital Assets or issuing Fiat stablecoins in or from the AIFC must be an Authorised Firm licensed by the AFSA for providing a Regulated Activity of Providing Money Services.

(2) A Person authorised to issue Fiat stablecoins may provide Money Services in relation to Digital Assets and Money Services under paragraph 21 Schedule 1 GEN.

Guidance: Authorisation

Under GLO Providing Money Services in relation to Digital Assets means providing of Money Service of buying and selling of Digital Asset, as well as providing Money Services provided under paragraph 21 Schedule 1 GEN, including with the use of Digital Assets.

### 4.1.-1. Providing Money Services in relation to Digital Assets

(1) An Authorised Firm Providing Money Services in relation to Digital Assets or issuing Fiat stablecoins may use Digital Assets in connection with providing Money Services under paragraph 21 Schedule 1 GEN if the Digital Asset:

(a) has been approved by the AFSA in accordance with PMS 2.4.1 (2); and

(b) used only for the purposes of providing Money Services;

(2) In subrule (1) Digital Asset may be directly sent to or received from the Client or sent, received and held in the Client's name.

### 4.2. Requirements

The AFSA may not grant authorisation or variation of a Licence to carry on the activities of Providing Money Services in relation to Digital Assets or issuing Fiat stablecoins if:

(a) the applicant does not meet general authorisation requirements under the Framework Regulations and other applicable rules, and

(b) the applicant does not have capital of at least USD 200,000. In the case of a Person applying for authorisation for the activities of Providing Money Services in relation to Digital Assets or issuing Fiat stablecoins in addition to conducting another Regulated Activity for which the capital requirement is higher than USD 200,000, the highest amount applies.

An Authorised Firm carrying on activities, including Providing Money Services, in relation to Digital Assets cannot carry on Regulated Activities in relation to other Investments unless it obtains written approval from the AFSA.

### 4.3. Mandatory appointments

In addition to the mandatory appointments required by GEN 2.1, an Authorised Person Providing Money Services in relation to Digital Assets must appoint a Chief Information Technology Officer, who is an individual responsible for its ongoing information technology ("IT") operations, maintenance and security oversight to ensure that the Authorised Firm's IT systems are reliable and adequately protected from external attack or incident.

### 4.4 Governance arrangements

(1) A Digital Asset Service Provider must have robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks to which it is or might be exposed, and adequate internal control mechanisms, including sound administrative and accounting procedures.

(2) A Digital Asset Trading Facility Operator must have an effective Board of Directors which is collectively accountable for ensuring that the Digital Asset Trading Facility Operator's business is managed prudently and soundly. At least one-third of the Board of Directors should comprise independent Directors.

*Note: Rule 4.4 (2) will come into force 12 months after the commencement of these Rules.*

(3) Members of the Governing Body of the Digital Asset Service Provider must have sufficiently good repute and possess sufficient knowledge, experience, and skills to perform their duties. They must also demonstrate that they are capable of committing sufficient time to effectively perform their duties.

(4) Members of the Governing Body of the Digital Asset Service Provider that issues a Fiat or Commodity stablecoin (an "issuer of a Fiat stablecoin or Commodity stablecoin") must ensure effective and prudent management of the reserve of assets. The issuer of a Fiat stablecoin or Commodity stablecoin must ensure that issuance and redemption of a Fiat stablecoin or Commodity stablecoin is always matched by a corresponding increase or decrease of the reserve of assets.

## 4.5 Policies and procedures

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must establish, maintain and implement policies and procedures on:

(a) the reserve of assets, including how the reserve assets will be invested and held as applicable;

(b) the custody of the reserve assets, including the segregation of assets;

(c) the rights or the absence of rights granted to the holders of Fiat stablecoins or Commodity stablecoins, as specified in DAA 4.11.2;

(d) the mechanism through which Fiat stablecoins or Commodity stablecoins are issued and redeemed;

(e) the protocols for validating transactions in Fiat stablecoins or Commodity stablecoins;

(f) the functioning of the issuer of a Fiat stablecoin or Commodity stablecoin's proprietary DLT, where the Fiat stablecoins or Commodity stablecoins are issued, transferred and stored on such DLT or similar technology that is operated by the issuer of a Fiat stablecoin or Commodity stablecoin or a third party acting on its behalf;

(g) the mechanisms to ensure the liquidity of Fiat stablecoins or Commodity stablecoins;

(h) the arrangements with third parties, including for managing the reserve assets and the investment of the reserve, the custody of reserve assets, and, where applicable, the distribution of Fiat stablecoins or Commodity stablecoins to the public;

(i) the written consent of the issuer of the Fiat stablecoin or Commodity stablecoin given to Persons who may offer or admit to trading the Fiat stablecoin or Commodity stablecoin;

(j) business continuity and operational resilience, including having in place a business continuity policy and contingency plan;

(k) the plan that ensures, in case of an interruption of its systems and procedures, the preservation of essential data and functions and the maintenance of its activities, or, where that is not possible, the timely recovery of such data and functions and the timely resumption of its activities;

(l) the stabilisation mechanism which must in particular:

(i) list the reference assets in relation to which a Fiat stablecoin or Commodity stablecoin aims at stabilising its value and the composition of such reference assets; and

(ii) describe the type of assets and the precise allocation of assets that are included in the reserve of assets;

(iii) contain a detailed assessment of the risks, including credit risk, market risk, concentration risk and liquidity risk resulting from the reserve of assets;

(iv) describe the procedure by which a Fiat stablecoin or Commodity stablecoin is issued and redeemed, and the procedure by which such issuance and redemption will result in a corresponding increase and decrease in the reserve of assets;

(v) mention whether a part of the reserve of assets is invested as provided in DAA 4.7.4;

(vi) describe the procedure to purchase a Fiat stablecoin or Commodity stablecoin and to redeem such stablecoin against the reserve of assets, and list the persons or categories of persons who are entitled to do so.

(m) complaint handling;

(n) conflicts of interests;

(o) recovery and winddown; and

(p) the management of reserve assets and the liquidity risks associated with redemptions.

(2) The policies and procedures required by DAA 4.5.1(n) must include an independent audit to be conducted by a third party at least annually to assess: (i) whether the amount required to achieve recovery and orderly winddown is set out in the policy; and (ii) whether that amount is sufficient.

## 4.6. Technology governance, controls and security

### 4.6.1. Systems, controls and procedures

(1) A Digital Asset Service Provider must ensure that it implements systems and controls necessary to address the risks, including cybersecurity-related risks, to its business.

The relevant systems and controls should take into account such factors that include the nature, scale and complexity of the Digital Asset Service Provider's business, the diversity of its operations, the volume and size of its business and the level of risk inherent in its business.

(2) A Digital Asset Service Provider must have adequate systems and controls to enable it to calculate and monitor its capital resources and its compliance with the requirements in DAA 4.2. The systems and controls must be in writing and must be appropriate for the nature, scale and complexity of the Digital Asset Service Provider's business and its risk profile.

(3) A Digital Asset Service Provider must employ appropriate and proportionate systems, resources, and procedures to ensure the continued and regular performance of its services and activities.

(4) If the issuer of a Fiat stablecoin or Commodity stablecoin decides to discontinue providing services and activities, such as issuing the Fiat stablecoin or Commodity stablecoin, the issuer of a Fiat stablecoin or Commodity stablecoin must present a plan to the AFSA for such discontinuation, for the AFSA's approval, and comply with any requirements imposed by the AFSA in relation to such discontinuation.

(5) Issuer of a Fiat stablecoin or Commodity stablecoin must identify sources of operational risks and minimise those risks through the development of appropriate systems, controls and procedures.

(6) Issuer of a Fiat stablecoin or Commodity stablecoin must have internal control mechanisms and effective procedures for risk management.

**4.6.1.-1. Risk warnings**

(1) An Authorised Firm Providing Money Services in relation to Digital Assets and issuing Fiat stablecoins must display prominently on its website the following risk warnings relating to Digital Assets:

(a) except in the case of a Central Bank Digital Currency, Digital Assets are not legal tender or backed by a government;

(b) Digital Assets are subject to extreme volatility, and the value of the Fiat stablecoins can fall quickly (including, in respect of a Fiat stablecoin or Commodity stablecoin, if it loses its stability peg);

(c) that Digital Assets may not always be liquid or transferable;

(d) that Digital Assets can be stolen because of cyberattacks;

(e) that the nature of Digital Assets may lead to an increased risk of Financial Crime;

(f) there are limited or, in some cases, no mechanisms available for the recovery of lost or stolen Digital Assets;

(j) the risks of Digital Assets with regard to anonymity, irreversibility of transactions, accidental transactions, transaction recording, and settlement;

(h) that the nature of Digital Assets means that technological difficulties experienced by an Authorised Firm Providing Money Services in relation to Digital Assets or a Digital Asset Service Provider may prevent access to or use of a Client's Digital Assets;

(i) that there is no recognised compensation scheme to provide an avenue of redress for aggrieved participants.

(2) Where an Authorised Firm Providing Money Services in relation to Digital Assets presents any marketing or educational materials, or and other communications relating to a Digital Assets, approved in accordance with subrule (1), whether on a website, in the general media or as part of a distribution made to existing or potential new Clients, it must include the risk warning referred to in subrule (1) in a prominent place at or near the top of each page of the materials or communication.

(3) If the materials referred to in (1) is provided on a website or an application that can be downloaded to a mobile device, the warning must be:

(a) statically fixed and visible at the top of the screen, even when a person scrolls up or down the webpage; and

(b) included on each linked webpage on the website.

(c) provided before final confirmation of any transaction.

### 4.6.2. Technology governance and risk assessment framework

(1) A Digital Asset Service Provider must implement a technology governance and risk assessment framework which must be comprehensive and proportionate to the nature, scale, and complexity of the risks inherent in their business model.

(2) The technology governance and risk assessment framework must apply to all technologies relevant to a Digital Asset Service Provider's business and clearly set out the Digital Asset Service Provider's cybersecurity objectives.

(3) A Digital Asset Service Provider must ensure that its technology governance and risk assessment framework is capable of determining the necessary processes and controls that it must implement in order to adequately mitigate any risks identified.

(4) A Digital Asset Service Provider must ensure that its technology governance and risk assessment framework addresses appropriate governance policies and system development controls, such as a development, maintenance and testing process for technology systems and operations controls, back-up controls, capacity and performance planning and availability testing.

### 4.6.3. Cyber-security matters

A Digital Asset Service Provider must take reasonable steps to ensure that its IT systems are reliable and adequately protected from external attack or incident.

### 4.6.4. Cyber-security policy

(1) A Digital Asset Service Provider must create and implement a policy which outlines their procedures for the protection of its electronic systems.

(2) A Digital Asset Service Provider must ensure that its cyber-security policy is reviewed at least annually by its Chief Information Technology Officer.

(3) The cyber-security policy must, as a minimum, address the following areas:

(a) information security;

(b) data governance and classification;

(c) access controls;

(d) capacity and performance planning;

(e) systems operations and availability concerns;

(f) systems and network security, consensus protocol methodology, code and smart contract validation and audit processes;

(g) systems and application development and quality assurance;

(h) physical security and environmental controls, including procedures around access to premises and systems;

(i) customer data privacy;

(j) procedures regarding the facilitation of Digital Asset transactions initiated by a Client including considering multi-factor authentication or any better standard for Digital Asset transactions that—

(i) exceed transaction limits set by the Client, such as accumulative transaction limits over a period of time; and

(ii) are initiated after a change of personal details by the Client, such as the address of a Digital wallet;

(k) procedures regarding Client authentication and session controls including the maximum incorrect attempts for entering a password, appropriate time-out controls and password validity periods;

(l) procedures establishing adequate authentication checks when a change to a Client's account information or contact details is requested;

(m) vendor and third-party service provider management;

(n) monitoring and implementing changes to core protocols not directly controlled by the Digital Asset Service Provider;

(o) incident response, including root cause analysis and rectification activities to prevent reoccurrence;

(p) governance framework and escalation procedures for effective decision-making and proper management and control of risks and emergency incidents, including responses to ransomware and other forms of cyberattacks; and

(q) hardware and infrastructure standards, including network lockdown, services/desktop security and firewall standards.

## 4.7. Reserve of assets

### 4.7.1. Requirements related to a reserve of assets

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must make reserve assets available for examination and for verification of the issuer of a Fiat stablecoin or Commodity stablecoin's disclosures on the AFSA's request.

(2) Issuer of a Fiat stablecoin or Commodity stablecoin must fully back such stablecoin with reserve assets, meaning that the value of the reserve assets must at all times be at least equal to the nominal value of all outstanding units of the Fiat stablecoin or Commodity stablecoin in circulation.

(3) Issuer of a Fiat stablecoin must issue stablecoins whose reserve assets consist of only one of the following fiat currencies ("reference assets"):

(a) Australian dollar;

(b) British pound sterling;

(c) Canadian dollar;

(d) Chinese yuan renminbi;

(e) European euro;

(f) Japanese yen;

(g) New Zealand dollar;

(h) Norwegian krone;

(i) Swedish krona;

(j) Swiss franc;

(k) United States dollar; or

(l) any other currency, except for Kazakhstani tenge, agreed with the AFSA.

(3-1) Issuer of a Commodity stablecoin must issue stablecoins whose reserve assets consist of referenced Commodities only.

(4) Issuer of a Fiat stablecoin or Commodity stablecoin must ensure that the reserve of assets is operationally segregated from the proprietary assets of the issuer of a Fiat stablecoin or Commodity stablecoin and from the reserve of assets of other Fiat stablecoins or Commodity stablecoins.

(5) The reserve of assets must be composed and managed in such a way that:

(a) the risks associated to the assets referenced by the Fiat stablecoin or Commodity stablecoin are covered; and

(b) the liquidity risks associated with the permanent redemption rights of the holders are addressed.

(6) Issuer of a Fiat stablecoin or Commodity stablecoin that offers two or more categories of Fiat stablecoins or Commodity stablecoins to the public must operate and maintain segregated pools of reserves of assets for each category of Fiat stablecoins or Commodity stablecoins. Each of these pools of reserve of assets must be managed separately.

(7) Issuer of a Fiat stablecoin or Commodity stablecoin must determine the aggregate value of reserve assets by using market prices. Their aggregated value must be at least equal to the aggregate value of the claims on the issuer of a Fiat stablecoin or Commodity stablecoin from holders of Fiat stablecoins or Commodity stablecoins in circulation.

(8) Issuer of a Fiat stablecoin or Commodity stablecoin must conduct monthly reconciliation of each Fiat stablecoin or Commodity stablecoin to demonstrate that the Fiat stablecoin or Commodity stablecoin is fully backed with reserve assets.

(9) The reconciliation must include the information that the issuer of a Fiat stablecoin or Commodity stablecoin meets requirements under DAA 4.7.1 and DAA 4.7.3.

**Guidance:**

If an issuer of a Fiat stablecoin accepts fiat currency from a Client in exchange for giving them Fiat stablecoins. The fiat currency held by the issuer would be considered as Client Money, and the issuer of a Fiat Stablecoin would need to comply with the Client Money provisions in the COB.

### 4.7.2. Independent audit

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must mandate an independent third party audit of the reserve assets annually but not later than four months after the close of its financial year.

(2) The result of the audit conducted under (1) must be provided to the AFSA without delay, at the latest within 4 weeks of the reference date of the valuation. The result of the audit must be published within three weeks of the date of the provision of the result of the audit to the AFSA.

(3) The AFSA may instruct the issuer of a Fiat stablecoin or Commodity stablecoin to delay the publication of the result of the audit in the event that:

(a) the issuer of a Fiat stablecoin or Commodity stablecoin has been required to implement a recovery arrangement;

(b) the issuer of a Fiat stablecoin or Commodity stablecoin has been required to implement a redemption plan;

(c) it is deemed necessary to protect the interests of holders of a Fiat stablecoin or Commodity stablecoin;

(d) it is deemed necessary to avoid a significant adverse effect on the financial system of the AIFC;

(e) the AFSA considers appropriate in pursuing the Regulatory Objectives.

(4) The valuation referred to in DAA 4.7.1 (7) at market prices must be made by using mark-to-market.

(5) When using mark-to-market:

(a) the reserve asset must be valued at the more prudent side of the bid and offer unless the reserve asset can be closed out at mid-market; and

(b) only good quality market data must be used. The issuer of a Fiat stablecoin or Commodity stablecoin must record the basis on which they deem market data of good quality, and ensure that such data is assessed on the basis of all of the following factors:

(i) the number and quality of the counterparties;

(ii) the volume and turnover in the market of the reserve asset; and

(iii) size of the reserve of assets.

(6) If the use of mark-to-market is not possible or the market data is not of sufficient quality, a reserve asset must be valued conservatively by using mark-to-model.

(7) The mark-to-model must accurately estimate the intrinsic value of the reserve asset, based on all of the following up-to-date key factors:

(a) the volume and turnover in the market of that reserve asset;

(b) the size of the reserve of assets; and

(c) market risk, interest rate risk, and credit risk attached to the reserve asset.

(8) When using mark-to-model, the amortised cost method must not be used.

### 4.7.3. Custody of reserve assets

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must establish, maintain and implement custody policies, procedures and contractual arrangements that ensure at all times that:

(a) the reserve assets are not encumbered nor pledged as Collateral;

(b) the reserve assets are held in custody;

(c) the issuer of a Fiat stablecoin or Commodity stablecoin has prompt access to the reserve assets to meet any redemption requests from the holders of Fiat stablecoins or Commodity stablecoins;

(d) concentration risk in the custody of reserve assets is mitigated and there is appropriate contingency planning in the event that a custodian is unable to perform its obligations;

(e) where appropriate concentration risks in the reserve assets are avoided; and

(e) there is proper due diligence of the robustness of the custodian used, including as regards ensuring that there is a credible and comprehensive wind-down plan in place for each custodian used.

(2) Issuer of a Fiat stablecoin or Commodity stablecoin that issues two or more categories of Fiat stablecoins or Commodity stablecoins must have a custody policy for each pool of reserve of assets.

(3) Issuer of a Fiat stablecoin or Commodity stablecoin must operate and maintain only one custody policy per category of Fiat stablecoin or Commodity stablecoin.

(4) The reserve assets must be held in custody by no later than 5 working days after the issuance of the relevant Fiat stablecoins or Commodity stablecoins.

(5) A Person providing custody services must be a Person different from the issuer of a Fiat stablecoin or Commodity stablecoin.

(6) Issuer of a Fiat stablecoin or Commodity stablecoin must ensure that a Person appointed as a custodian of the reserve assets has the necessary licences, expertise and market reputation to act as a custodian of such reserve assets, taking into account the accounting practices, safekeeping procedures and internal control mechanisms.

(7) The contractual arrangements between the issuer of a Fiat stablecoin or Commodity stablecoin and custodian must ensure that the reserve assets held in custody are protected against claims of the custodian's creditors.

(8) The custody policies and procedures referred to in (1) must set out the selection criteria for the appointments of custodians of the reserve assets and the procedure to review such appointments at least annually.

(9) A custodian of the reserve assets backing the Fiat stablecoin must comply with the rules relevant to Providing Custody, including those set out in chapter 8 of the COB (or, to the extent that the custodian is not based in the AIFC, in accordance with the rules of the jurisdiction of the custodian as well as any additional requirements which the AFSA may deem relevant to ensure that equivalent protections are in place as those provided by the Legal Framework provided by the AFSA).

(10) A custodian of the reserve assets backing the Commodity stablecoin must ensure that reserve assets are recorded, registered and held in an appropriate manner to safeguard and control such reserve assets.

(11) A custodian of the reserve assets backing the Commodity stablecoin must ensure compliance with any additional requirements which the AFSA may deem relevant to ensure that equivalent protections are in place.

### 4.7.4. Investment of reserve assets

(1) Issuer of a Fiat stablecoin must ensure that it has sufficient uninvested reserve assets to be able to meet the issuer of the Fiat stablecoin's ongoing obligations under DAA 4.7.1 at all times.

(2) The instruments which the issuer of a Fiat stablecoin invests the reserve assets into must be held in custody in accordance with DAA 4.7.3.

(3) Issuer of a Fiat stablecoin must hold at least 95% of reserve assets denominated in the reference assets in:

(a) cash or cash equivalents including central bank reserve deposits, bank deposits and Central Bank Digital Currency, which must comprise at least 30% of reserve assets; or

(b) highly liquid financial instruments with minimal market risk, credit risk, and concentration risk, which could be liquidated rapidly with minimal adverse market impact, including the following:

(i) debt securities with residual maturity of 90 days or less, issued by governments or central banks of the reference assets specified in DAA 4.7.1(3) or local or international government agencies;

(ii) repurchase agreements with a maturity of 7 or less which are backed by (i) above; and

(iii) short-term government money market funds.

(4) Issuer of a Fiat stablecoin may invest up to 5% of reserve assets in precious metals. If an issuer of a Fiat stablecoin invests in precious metals, a 20% haircut applies to such investment.

(5) All losses, including fluctuations in the value of the financial instruments referred to in (3), must be borne by the issuer of a Fiat stablecoin.

(6) All profits or losses and any counterparty or operational risks that result from the investment of the reserve of assets must be borne by the issuer of a Fiat stablecoin.

(7) If an issuer of a Fiat stablecoin invests a part of the reserve of assets, it must describe in detail the investment policy and contain an assessment of how that investment policy can affect the value of the reserve of assets.

(8) Issuer of a Fiat stablecoin must, at all times, manage reserve assets effectively and prudently, at least by:

(a) maintaining reserve assets only with custodians, as agreed with the AFSA during the authorisation process:

(i) appropriately and validly authorised to hold the specific type of reserve assets; and

(ii) that segregate reserve assets maintained by them from their own funds;

(b) ensuring newly added reserve assets are held in accordance with their custody arrangements;

(c) putting in place policies and procedures to ensure reserve assets can be promptly accessed and converted into the reference assets at all times, for the purpose of processing and completing any redemption requests in accordance with DAA 4.11.2; and

(d) conducting regular risk assessments to evaluate the appropriateness of the composition of reserve assets in ensuring compliance with DAA 4.7.1(2).

(9) Issuer of a Fiat stablecoin must insert provisions in their agreements with the relevant financial services firms to ensure the AFSA has priority access to reserve assets, to the further extent permitted by applicable laws, for the purposes of the AFSA fulfilling its regulatory obligations.

## 4.8. White paper

### 4.8.1. Content and form of the white paper

(1) A Digital Asset white paper for a Fiat stablecoin or Commodity stablecoin must contain all of the following information:

(a) information about the issuer of a stablecoin;

(b) information about the stablecoin;

(c) information on the rights and obligations attached to a stablecoin;

(d) information on the underlying technology used to operate the stablecoin;

(e) information on risks;

(f) information on the reserve of assets;

(g) the method and all factors used to calculate the value of reserve assets;

(h) the initial value and composition of the reserve assets;

(i) the conditions and the procedure to purchase stablecoins and redeem such stablecoins against reserve assets;

(j) details of the arrangements for the custody and management of the reserve assets;

(k) the rights provided to holders of the stablecoin;

(l) a summary of the redemption policies; and

(m) any other information that the AFSA requires.

(2) All information in the white paper referred to in (1):

(a) must be fair, clear and not misleading;

(b) must not contain material omissions; and

(c) must be presented in a concise and comprehensible form.

(3) The white paper must not contain any assertions on the future value of the Fiat stablecoin or Commodity stablecoin.

(4) The white paper must contain a clear and unambiguous statement that:

(a) the Fiat stablecoin or Commodity stablecoin may lose their value in part or in full;

(b) the Fiat stablecoin or Commodity stablecoin may not always be transferable; and

(c) the Fiat stablecoin or Commodity stablecoin may not be liquid.

(5) The white paper for a Fiat stablecoin or Commodity stablecoin must contain a statement from the management body of the issuer of a Fiat stablecoin or Commodity stablecoin confirming that the white paper complies with the requirements of this Rule and that, to the best knowledge of the management body, the information presented in the white paper:

(a) is in accordance with the facts; and

(b) makes no material omission likely to affect any decision to participate in the Fiat stablecoin or Commodity stablecoin.

(6) The white paper must contain a summary that in brief and non-technical language provides key information about the offer to the public of the Fiat stablecoin or Commodity stablecoin or about the intended admission of the Fiat stablecoin or Commodity stablecoin to trading on a Digital Asset Trading Facility.

(7) The summary must be presented and laid out in easily understandable words and in a clear and comprehensive form, using characters of readable size.

(8) The format and content of the summary of the white paper must provide, in conjunction with the white paper, appropriate information about the characteristics of the Fiat stablecoins or Commodity stablecoins concerned in order to help potential holders of the Fiat stablecoins or Commodity stablecoins to make an informed decision.

(9) The summary must indicate that:

(a) the holders of a Fiat stablecoin or Commodity stablecoin have a redemption right at any moment; and

(b) the conditions of redemption.

(10) The summary must contain a warning that:

(a) it should be read as an introduction to the white paper; and

(b) the potential holder should base any decision to purchase a Fiat stablecoin or Commodity stablecoin on the content of the whole white paper.

(11) Before the publication of the white paper no marketing communications or Financial Promotions can be made. This restriction does not affect the ability of the issuer of a Fiat stablecoin or Commodity stablecoin to conduct market soundings.

### 4.8.2. Modification of the white paper

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must inform in writing the AFSA of any intended change of the issuer of a Fiat stablecoin or Commodity stablecoin's business model likely to have a significant influence on the purchase decision of any actual or potential holder of a Fiat stablecoin or Commodity stablecoin, which occurs after the authorisation or approval of the white paper. Such changes may include:

(a) the governance arrangements, including reporting lines to the management body and risk management framework;

(b) the reserve assets and the custody of the reserve assets;

(c) the rights granted to the holders of a Fiat stablecoin or Commodity stablecoin;

(d) the mechanism through which Fiat stablecoins or Commodity stablecoins are issued and redeemed;

(e) the protocols for validating the transactions in Fiat stablecoins or Commodity stablecoins;

(f) the functioning of the issuer of a Fiat stablecoin or Commodity stablecoin's proprietary DLT, where the Fiat stablecoins or Commodity stablecoins are issued, transferred and stored on such a DLT;

(g) the mechanisms to ensure the liquidity of Fiat stablecoins or Commodity stablecoins, including the liquidity management policy for issuers of Fiat stablecoins or Commodity stablecoins;

(h) the arrangements with third parties, including for managing the reserve assets and the investment of the reserve, the custody of reserve assets, and, where applicable, the distribution of Fiat stablecoins or Commodity stablecoins to the public;

(i) the complaint handling procedure; or

(j) the money laundering and terrorist financing risk assessment and general policies and procedures.

(2) The AFSA must be informed in writing 30 working days before the intended changes take effect.

(3) The AFSA must grant its approval or refuse to approve the draft modified white paper within 30 working days following the acknowledgement of receipt.

(4) During the examination of the draft modified white paper, the AFSA may request an issuer of a Fiat stablecoin or Commodity stablecoin to provide any additional information, explanations or justifications on the draft modified white paper.

(5) If the AFSA requests additional information, the time limit of 30 working days must commence only when the AFSA has received the additional information requested.

(6) Where approving the modified white paper, the AFSA may require the issuer of Fiat stablecoins or Commodity stablecoins:

(a) to put in place mechanisms to ensure the protection of holders of Fiat stablecoins or Commodity stablecoins, when a potential modification of the issuer of a Fiat stablecoin or Commodity stablecoin's operations can have a material effect on the value, stability, or risks of the Fiat stablecoins or Commodity stablecoins or reserve assets;

(b) to take any appropriate corrective measures to address concerns related to financial stability, the smooth operation of payment systems, or market integrity.

**4.8.3. Liability of issuers of Fiat stablecoins or Commodity stablecoins for the information given in the white paper**

(1) If an issuer of a Fiat stablecoin or Commodity stablecoin or its management or supervisory bodies has breached requirements set out in DAA 4.8.1(2), by providing in its white paper or in a modified white paper information which is not complete, fair or clear or by providing information which is misleading, a holder of such Fiat stablecoins or Commodity stablecoins or bodies can claim for damage arising from the breach.

(2) To demonstrate that the issuer has breached DAA 4.8.1 (2), a holder of Fiat stablecoin or Commodity stablecoin must present evidence indicating that the issuer of Fiat stablecoins or Commodity stablecoins has breached DAA 4.8.1(2) and that such breach had an impact on the holder's decision to buy, sell or exchange the said Fiat stablecoin or Commodity stablecoin.

(3) No claim for damages arising from information provided in a summary (whether in its original form or as translated) may be made by a holder of Fiat stablecoins or Commodity stablecoins unless:

(a) the summary is misleading, inaccurate or inconsistent when read together with the other parts of the white paper; or

(b) the summary does not provide, when read together with the other parts of the white paper, key information in order to aid potential holders when considering whether to purchase such Fiat stablecoins or Commodity stablecoins.

**4.8.4. Publication of the white paper**

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must publish on its website its white paper as approved and as modified.

(2) The approved white paper must be publicly accessible by no later than the starting date of the offer to the public of the Fiat stablecoins or Commodity stablecoins or the admission of those tokens to trading on a Digital Asset Trading Facility.

(3) The approved white paper and the modified white paper must remain available on the issuer of a Fiat stablecoin or Commodity stablecoin's website for as long as the Fiat stablecoin or Commodity stablecoin is available to the public.

**4.9. AFSA power to limit the amount of Fiat stablecoins**

(1) The AFSA may limit the amount of Fiat stablecoins to be issued or impose a minimum denomination to the Fiat stablecoins if the National Bank of the Republic of Kazakhstan issues an opinion that the Fiat stablecoins pose a serious threat to monetary policy transmission, smooth operation of payment systems or monetary sovereignty. The AFSA may specify the applicable limit or minimum denomination amount.

(2) The AFSA may, at any time and in its sole discretion, prohibit or otherwise limit the issuance or use of a Fiat stablecoin before or after an issuer of a Fiat stablecoin which has been approved issues such Fiat stablecoin. The AFSA may require that any such issuer of a Fiat stablecoin delist, halt, or otherwise limit or curtail activity with respect to such Fiat stablecoin.

### 4.10. Monitoring of Fiat stablecoins or Commodity stablecoins

(1) If the AFSA considers it appropriate, it may require the issuer of a Fiat stablecoin or Commodity stablecoin to provide a report with the following information:

(a) the customer base, including details of the issuer of a Fiat stablecoin or Commodity stablecoin's customer base which must include a breakdown of the type of customer by reference to their category, size, type and geographical distribution;

(b) the value of the Fiat stablecoins or Commodity stablecoins issued and the size of the reserve of assets;

(c) the average number and value of issuances and redemption requests per day; and

(d) information that the AFSA requires.

(2) Digital Asset Service Providers, which provide services in relation to Fiat stablecoins or Commodity stablecoins, must make reasonable efforts to provide the issuer of a Fiat stablecoin or Commodity stablecoin with information necessary to prepare the report, including by reporting off chain transactions.

### 4.11. Miscellaneous

#### 4.11.1. Ongoing information to holders of Fiat stablecoins or Commodity stablecoins

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must in a clear, accurate and transparent manner disclose at least once a quarter, on a publicly and easily accessible place on its website, the amount of Fiat stablecoins or Commodity stablecoins in circulation, and the value and the composition of the reserve assets.

(2) In case of a Fiat stablecoin, the published information must demonstrate that the reserve assets:

(a) are at least equal in value to the notional value of outstanding Fiat stablecoins in circulation (that value is calculated by multiplying the number of Fiat stablecoins in circulation by the purported pegged Fiat Currency value);

(b) are denominated in the reference currency; and

(c) are held in segregated accounts with properly regulated custodians.

(3) Issuer of a Fiat stablecoin or Commodity stablecoin must publish as soon as possible on a publicly and easily accessible place on its website a brief, clear, accurate and transparent summary of the audit report and the full and unredacted audit report in relation to the reserve assets.

(4) Issuer of a Fiat stablecoin or Commodity stablecoin must as soon as possible and in a clear, accurate and transparent manner disclose on its website any event that has or is likely to have a significant effect on the value of the Fiat stablecoin or Commodity stablecoin, or on the reserve assets.

### 4.11.2. Redemption rights

(1) Issuer of a Fiat stablecoin or Commodity stablecoin must grant holders redemption rights at all times on the issuer of a Fiat stablecoin or Commodity stablecoin, and on the reserve assets when the issuer is not able to comply with its obligations.

(2) Holders should be able to redeem their Fiat stablecoins or Commodity stablecoins at any moment and at par value against the referenced asset, by delivering the assets backing the Commodity stablecoins or other means approved by the AFSA.

(3) Issuer of a Fiat stablecoin or Commodity stablecoin must ensure that all requests made by holders, with valid client agreements with the issuer of a Fiat stablecoin or Commodity stablecoin, to redeem the Fiat stablecoin or Commodity stablecoin are processed and completed:

(a) promptly and no later than 5 working days of any such requests, in case of a Fiat stablecoin, or within reasonable timeframe, in case of a Commodity stablecoin; or

(b) if the trading or settlement of the reserve assets is subject to significant disruption events beyond the control of an issuer of a stablecoin, promptly and no later than 5 working days of the trading or settlement of reserve assets no longer being significantly impacted by such disruption events, in case of a Fiat stablecoin, or within reasonable timeframe, in case of a Commodity stablecoin.

(4) Issuer of a Fiat stablecoin or Commodity stablecoin is allowed to charge a reasonable fee for processing and completing redemption requests. The redemption fee must be clearly disclosed on the website of the issuer of a Fiat stablecoin or Commodity stablecoin and must be proportionate and commensurate with the actual costs incurred by the issuer of a Fiat stablecoin or Commodity stablecoin in completing the redemption request.

(5) Issuer of a Fiat stablecoin or Commodity stablecoin must establish, maintain and implement clear and detailed policies and procedures setting out:

(a) the conditions, including thresholds, periods and timeframes, for holders of a Fiat stablecoin or Commodity stablecoin to exercise this right;

(b) the mechanisms and procedures to ensure the redemption of the Fiat stablecoins or Commodity stablecoins;

(c) the valuation, or the principles of valuation, of the Fiat stablecoins or Commodity stablecoins and of the reserve assets when this right is exercised by the holder of a Fiat stablecoin or Commodity stablecoin;

(d) the settlement conditions when this right is exercised; and

(e) measures the issuer of a Fiat stablecoin or Commodity stablecoin is taking to adequately manage increases or decreases of the reserve, to avoid any adverse impacts on the market of the assets included in the reserve.

### 4.11.3. Ongoing capital

(1) In addition to DAA 4.2(b), an issuer of a Fiat stablecoin or Commodity stablecoin must ensure that it maintains at all times ongoing capital resources in the amount of 2% of the average outstanding Fiat stablecoins or Commodity stablecoins in relation to each category of Fiat stablecoin or Commodity stablecoin issued by it.

(2) The ongoing capital referred to in 4.11.3(1) should consist of the Common Equity Tier 1 items and instruments.

(3) If an issuer of a Fiat stablecoin or Commodity stablecoin offers more than one category of Fiat stablecoins or Commodity stablecoins, the amount of the average outstanding Fiat stablecoins or Commodity stablecoins should be the sum of the average amounts of the reserve assets backing each category.

**Guidance:**

The term ‘average outstanding Fiat stablecoins or Commodity stablecoins’ refers to the average amount of reserve assets at the end of each calendar day, calculated over the preceding 6 (six) months. If the relevant period does not exceed 6 (six) months, an issuer of a Fiat stablecoin or Commodity stablecoin should calculate the average outstanding Fiat stablecoins or Commodity stablecoins based on the actual data.

### 4.11.4. Prohibitions

(1) Issuer of a Fiat stablecoin or Commodity stablecoin is prohibited from granting any interest to holders of the Fiat stablecoin or Commodity stablecoin.

(2) For the purposes of this Rule, any remuneration or any other benefit related to the length of time during which a holder of a Fiat stablecoin or Commodity stablecoin holds such a Fiat stablecoin or Commodity stablecoin must be treated as interest.

(3) The interest includes net compensation or discount, with an equivalent effect of an interest received by the holder, directly from the issuer or through third parties, directly associated with the Fiat stablecoin or Commodity stablecoin or through the remuneration or pricing of other products.

(4) The issuance of stablecoins that aim or purport to maintain a stable value via protocols that provide for the increase or decrease of the supply of such stablecoins or other digital assets in response to changes in demand is prohibited.