CLIENT ASSET SAFEGUARDING POLICIES AND PROCEDURES

DOCUMENT OWNER	**Mask Virtual Assets Exchange LLC (THE "COMPANY")**
REPORT PREPARED BY	**BRYAN LEE - LEGAL & COMPLIANCE**
LAST REVIEWED DATE	**19.11.2025**
APPLICABLE TO	**MASK VIRTUAL ASSETS EXCHANGE L.L.C.**

Update Log:

Version	Date	Creator
Ver 1.0	14.9.2023	Bryan Lee / Daniel Tan
Ver 2.0	2.1.2024	Bryan Lee
Ver 3.0	25.07.2024	Nipun Sangeeth
Ver 3.1	20.09.2024	Nipun Sangeeth
Ver 3.2	04.02.2025	Awatef Ismail
Ver 3.3	16.06.2025	Bryan Lee
Ver 3.3	19.11.2025	Bryan Lee

1. INTRODUCTION

1.1 Background and Purpose of the Policy

(a) In the rapidly evolving landscape of digital finance, safeguarding client assets, particularly digital assets (hereafter "**VA**" or "**VAs**" or "**Virtual Assets**"), is of paramount importance. Our Client Asset Safeguarding Policies and Procedures are designed to ensure the highest level of security, transparency, and trust in the management of your digital assets.

(b) As such, Mask Virtual Assets Exchange LLC (hereafter "**MetraCore**", "**Us**", "**We**", "**Our**" and "**Company**") has appointed Hex Trust MENA FZE, a company incorporated in Dubai, having its registered office at Office #08-120, 8th Floor, The Offices 4, One Central, Dubai, United Arab Emirates (hereafter "**Hex**", "**Hex Trust**" and "**Custodian**") as the official custodian in reference to the custody agreement signed between on Us and the Custodian on 2 February 2024 and the Custodian Handbook issued by Hex Trust from time to time, which sets out the operative procedural rules for instructions, user roles, vault structures, and approval matrices.

(c) As a trusted custodian in the cryptocurrency space, Hex Trust is committed to implementing robust measures that protect its users (hereafter "**User**", "**Customer**" and "**Client**") assets from potential risks. These policies outline the meticulous steps we take to segregate, manage, and secure your assets, reflecting our dedication to maintaining the integrity and confidentiality of your holdings.

(d) Hex Trust's robust approach is grounded in industry best practices and compliance with regulatory requirements, ensuring that User's assets are not only safeguarded but also managed with the utmost professionalism and care. Hex Trust employs a combination of advanced technological solutions and stringent operational protocols to provide a secure environment for your digital assets.

(e) This policy provides a comprehensive overview of Our safeguarding policies, detailing the specific procedures We and the Custodian have in place to ensure the safety and proper management of client assets. From account segregation and record-keeping to asset storage and auditing, every aspect of our policy framework is designed to deliver unparalleled security and peace of mind to our clients.

(f) By adhering to these policies, we aim to foster a transparent and secure ecosystem where clients can confidently entrust us with their digital assets, knowing that they are protected by rigorous standards and practices.

1.2 Regulatory Framework

(a) We adhere to applicable regulations. This policy is crafted to ensure full compliance with mandates while also setting a benchmark for best practices in asset safeguarding within the industry. As regulatory guidelines evolve, this policy will undergo periodic reviews and updates to reflect the most current standards and practices.

2. OBJECTIVES

2.1 **The principal objectives of this policy are as follows**.

2.2 Asset Protection

To ensure the utmost security and protection of all client assets, especially Virtual Assets, against potential threats, misappropriation, and unauthorized access.

2.3 Regulatory Compliance

To guarantee full compliance with all pertinent regulations and directives set forth by the Virtual Assets Regulatory Authority ("**VARA**") and other applicable regulatory bodies in the UAE.

2.4 **Transparency**

To foster a transparent environment where Clients are consistently informed about the status, location, and management procedures related to their assets.

2.5 Operational Excellence

To institute best practices and standards for the effective management and oversight of Client assets, ensuring that they are handled with diligence, care, and precision.

2.6 Client Trust

To enhance and maintain the trust of our Clients by demonstrating unwavering commitment to the security, integrity, and proper management of their assets.

2.7 Continuous Improvement

To regularly review, assess, and update our asset safeguarding procedures in alignment with technological advancements, evolving regulatory landscapes, and best industry practices.

2.8 **Internal Awareness and Training**

To ensure that all relevant personnel are adequately trained, regularly updated, and aligned with this policy's guidelines and the broader regulatory framework.

3. SCOPE

3.1 This policy applies to the entire spectrum of assets that the Company holds, manages, or controls on behalf of Our Clients. For clarity and specificity, the assets covered under this policy are categorised as follows:

3.2 Virtual Assets

Virtual Assets, as defined by the VARA and for the purpose of this policy, encompass:

(a) **Direct Holdings**: Virtual Assets directly held by the Company in an account or VA Wallet.

(b) **Named Assets**: Virtual Assets held in an account or VA Wallet in the Company's name.

(c) **Controlled Entities**: Virtual Assets held by a legal entity or in an account or VA Wallet in the name of a legal entity that is controlled by the Company.

(d) **Key Management**: Situations where the private keys and/or seed phrase of the VA

Wallet are held or controlled by the Company.

3.3 Tangible Assets:

Physical assets, such as property, equipment, or other valuables, that may be held in trust or as collateral on behalf of Clients.

3.4 Intangible Assets:

These can include intellectual property rights, patents, copyrights, or other non-physical assets held or managed on behalf of Clients.

3.5 Exclusions

Assets immediately due and payable to the Company for the Company's own account, such as fees for services provided to a Client, amounts payable by the Company for expenses incurred on behalf of the Client, and other charges that are due and payable to the Company, are not considered as Client assets under this policy. This policy's scope ensures a holistic approach to safeguarding Client assets while emphasizing the unique characteristics and requirements of managing Virtual Assets. It serves as the foundation for the subsequent sections, which detail the policy statements and procedures.

4. DEFINITIONS

4.1 For the purposes of the policy, the following terms are defined as:

(a) **Client Virtual Assets**: Virtual Assets held or controlled by a VASP on behalf of a Client in the course of, or in connection with, any VA Activity. Exclusions include Virtual Assets immediately due and payable to a VASP for its own account (such as service fees), amounts payable by the VASP for expenses incurred on the Client's behalf, and other due and payable charges to the VASP.

(b) **Virtual Asset Service Providers** (herein referred to as "**VASP**"): Entities or individuals that conduct activities or operations for or on behalf of a customer, concerning buying/selling, exchange, transfer, or storage of Virtual Assets. VASPs include, but are not limited to, exchanges, wallet providers, and financial service providers for Virtual Assets.

(c) **VA Wallet**: A software or hardware mechanism that allows its owner to store, retrieve, and manage the private keys associated with their Virtual Assets. VA Wallets can be categorised as:

(i) **Warm Wallet**: A VA Wallet that is connected to the internet on a limited or controlled basis, typically used for operational needs that require routine transactions.

(ii) **Hot Wallet**: A VA Wallet that is connected to the internet and is meant for routine transactions.

(iii) **Cold Wallet**: A VA Wallet that remains offline, offering enhanced security against online hacks and is typically used for storing large amounts of Virtual Assets for extended periods.

5. POLICY STATEMENTS

5.1 Treatment of Client Virtual Assets

(a) **Systematic Framework**: Our Company is committed to establishing, implementing, and periodically reviewing policies, systems, and controls that are suitable for the nature and scale of our operations, ensuring optimal protection of Client VAs.

(b) **Liability Clarification**: We recognize Client VAs neither as our depository liabilities nor assets. They remain the exclusive property of the Client and are held in trust by our Company. Client VAs are not owned by the Company and shall not form part of the Company's estate in the event that the Company is or becomes insolvent.

(c) **Asset Segregation**: We shall store and manage Client VAs in VA Wallets or accounts distinctly separate from those holding our Company's own Virtual Assets, preventing any commingling of funds. We shall ensure that all Client VAs are held in separate VA Wallets from the Company's own VAs at all times, and each VA Wallet holding Client VAs shall be clearly designated as a "Client VA Wallet" in the Company's books, records, and internal wallet management systems. Each VA Wallet holding Client Virtual Assets under the Custodian arrangement shall be clearly identified and designated as a client wallet in the Custodian's and the Company's records and internal wallet management systems, in line with the Custodian Handbook.

(d) **Rehypothecation**: Our Company prohibits the rehypothecation of Client VAs unless explicit prior consent has been obtained from the Client, ensuring alignment with regulatory guidelines and our internal controls.

(e) **Asset Proceeds**: We are dedicated to ensuring that proceeds related to Client VAs, such as airdrops or staking gains, accrue to the Client's benefit. Any variations from this stance will be based on explicit agreements with the Client.

5.2 Proof of Reserves

(a) **Compliance with Reserve Assets**: We align with the Reserve Assets requirements and are committed to ensuring that our held assets in 1:1 reserve adequately cover all Client VA obligations.

(b) **Licensing Stipulations**: We will adhere to any additional stipulations presented by VARA during the licensing process or other periodic assessments, fostering transparency and accountability.

5.3 Reconciliation (Please note that the regulated custodian conducts the current reconciliation)

(a) **Daily Reconciliation**: Our Company commits to maintaining a rigorous daily reconciliation system for each Client's Virtual Assets, encompassing both credit and debit ledger balances.

(i) On-Chain Segregation: Each Client's assets are stored in individually segregated wallets on-chain. Since each wallet is distinct and tied to a specific Client, the balances of these wallets can be easily verified by querying the blockchain.

(ii) Automated Reconciliation Tools: Hex Trust integrates computerized tools to

track transactions and balances in real-time. These tools compare on-chain data with the internal ledger, ensuring that all assets held within Hex Trust's custody match the blockchain records.

(iii) API Integration: Hex Trust's systems can be integrated with Clients' internal systems via APIs, allowing for continuous updates of balances and transaction history. This enables automated and real-time reconciliation of the assets without manual intervention.

(iv) Auditing and Reporting: Automated reports are generated regularly, comparing the on-chain balance of each client's wallet with the internal record. Discrepancies, if any, are flagged and investigated promptly to ensure the integrity of the assets held in custody.

(b) **Discrepancy Reporting**: In the event of any material discrepancies during reconciliation that remain unresolved, we will promptly notify VARA in line with established protocols.

5.4 Segregation, Record Keeping, Oversight, and Client Communication

(a) **Segregation**: We maintain a clear separation between Client assets and our Company's proprietary assets, ensuring distinct and transparent records for each. This segregation is also maintained by ensuring separate wallets for holding Client VAs and the Company's proprietary VAs.

(b) **Record Keeping**: Our Company will maintain comprehensive, secure, and organized records of all Client VAs and their transactions, facilitating audits and swift retrieval.

(c) **Oversight**: We will conduct regular internal reviews and audits, ensuring compliance with these policies, regulatory directives, and industry best practices.

(d) **Client Communication**: Transparency is paramount, and we are dedicated to regularly updating our clients about the status, management, and notable actions related to their assets.

6. OVERVIEW OF THE WALLET INFRASTRUCTURE

6.1 The Company's current Hex Trust vault configuration comprises a dedicated custodial infrastructure designed exclusively for safeguarding Client Virtual Assets ("**Client VAs**"). All Client VAs are stored within wallets operated entirely by Hex Trust, segregated across cold, warm, and hot wallet environments. These wallets serve distinct operational and security purposes and are used solely for Client VAs. They remain completely isolated from any Company proprietary assets to ensure full segregation and compliance with regulatory safeguarding requirements.

6.2 The Company's current Hex Trust vault configuration is as follows:

(a) **Wallets holding Client VAs**: All Client VAs are held within a dedicated wallet infrastructure operated exclusively by Hex Trust, as further detailed in this policy. Client assets are segregated across cold, warm, and hot wallets, each serving specific operational and security purposes. These wallets are used solely for Client VAs and are completely isolated from any Company proprietary assets. The Company utilises three categories of custodial wallets

under its Hex Trust Enterprise:

(i) **Hot Wallet (Safe Vault – 0 out of 1 Approval Scheme):** Hot wallets are operated through Hex Trust's Safe Vault environment under a zero-approval scheme (0-out-of-1) and are used for high-frequency automated withdrawals that require immediate liquidity.

(ii) **Warm Wallet (Safe Vault – 1 out of 1 Approval Scheme):** Warm wallets are also maintained within Safe vaults but under a one-approval scheme (1-out-of-1), and they provide controlled operational liquidity for routine withdrawals and internal transfers.

(iii) **Cold Wallet (Safe Plus Vault – 1 out of 1 Approval Scheme):** Cold wallets, which represent the high-security layer where at least 90 % of Client VAs are stored, are operated through Hex Trust's Safe Plus vault environment. These cold wallets are fully air-gapped, utilising one-way data diodes to ensure complete isolation from online systems, and they require manual release by a Hex Trust operator after the Company's Initiator and Approver have authorised a transaction.

(b) **Wallets holding Company VAs**: The Company's proprietary virtual assets ("Company VAs") are maintained separately in Company-owned hot wallets. These wallets store only Company assets, including but not limited to trading-related revenues, fees, and other operational balances. Under no circumstances are Company VAs and Client VAs commingled. This strict segregation ensures:
(i) Clear operational separation between Company and Client VAs;
(ii) Accurate accounting and asset traceability; and
(iii) Compliance with all safeguarding, custody, and regulatory requirements under the VARA Regulations.

6.3 The Company's Client VA wallets are maintained on an omnibus basis, meaning that Client VAs are pooled within shared custody wallets while remaining fully segregated on the Company's internal ledger. These wallets are expressly designated as "Client VA Wallets" in both Hex Trust's systems and in the Company's own books and records. At no point are Client VAs commingled with Company proprietary virtual assets. The Company's proprietary assets ("Company VAs") are held separately in Company-owned hot wallets that contain only corporate balances such as fee revenue, trading income, or operating funds. This strict separation ensures robust auditability, regulatory compliance, and the clear demarcation of Client assets from Company assets.

6.4 Private key lifecycle management for all Client VA wallets is performed exclusively by Hex Trust. Keys are generated inside certified Hardware Security Modules ("HSMs") using a True Random Number Generator, ensuring that private keys never appear in plaintext and never leave the secure boundaries of the HSM. Hex Trust employs a multi-shard, multi-site encrypted backup architecture, distributing encrypted key shards across several secure physical vaults. Reconstruction of private keys requires a quorum of shards in accordance with Hex Trust's threshold security scheme, and neither the Company nor its personnel have access to any shard or key-reconstruction process. Signing operations for all Client VA transactions occur strictly within the HSM through Hex Trust's

Key Management System. For Safe Plus cold vaults, the final release requires manual action by a Hex Trust operator following Company Initiator and Approver authentication via the Hex Trust Mobile App. For Safe warm and hot wallets, transaction releases occur automatically once the required approval and policy-engine rules are met.

7. PROCEDURES

7.1 Modus Operandi for Liquidity

(a) The Company is committed to guaranteeing the protection of Client VAs, while also ensuring the sufficient liquidity is maintained at all times.

(b) Of the assets deposited into a Client's account, the Company, via the Custodian, utilises a risk-based allocation between:

(i) **Safe Plus vaults** (Cold Wallet) for long-term, higher-security storage; and

(ii) **Safe vaults** (Warm Wallet and Hot Wallet) for operational liquidity.

The specific vault allocations, approval schemes and limits are set out in the Custodian Handbook (including the current structure of Metra Warm Wallet – Safe, 1 out of 1; Metra Cold Wallet – Safe Plus, 1 out of 1; Hot Wallet – Safe, 0 out of 1), and may be updated by the Custodian from time to time.

(c) Both cold and warm wallets utilize advanced security technology, including air-gapped Hardware Security Modules ("**HSM**") to store private keys securely. The HSM employs Cross Domain Solutions ("**CDS**") with data diodes to ensure a one-way data flow, preventing any leakage from the secure environment. Importantly, at no point do private keys leave the HSM, ensuring the highest level of security for client assets.

(d) Neither the Custodian nor the Company may move Client VAs except pursuant to valid instructions given by the Company's Authorised Users (as defined and listed in the Custodian Handbook) or, where applicable, pursuant to instructions given under a Master Trading Agreement for OTC trades or as explicitly mentioned in this policy in the withdrawal process. For Safe Plus vaults, the final release step is performed by a Hex Trust operator; for Safe vaults, release may be automated once all policy engine criteria and approval quorums are met.

(e) Additionally, the Company will implement clear communication protocols with Hex Trust to continuously monitor the balance of VAs in cold and warm wallets. In collaboration with other relevant teams, the compliance team will conduct periodic reviews to ensure that liquidity requirements are met, thus maintaining operational integrity and safeguarding against potential disruptions.

(f) The current setup as described in this policy is based on a risk-based approach to address potential threats such as hacking, and may evolve as the Company's operations scale. The liquidity management approach will be reviewed and adapted as necessary to meet the operational demands effectively.

7.2 Treatment Procedures for Client VAs

(a) **Asset Deposits**:

(i) All incoming Client VAs are to be immediately verified against transaction details provided by clients.

(ii) Client VAs are deposited to vault-level deposit addresses (i.e. per vault + per asset).

(iii) An automated alert system is in place to notify the responsible team of any new deposits.

(b) **Error Identification and Correction**:

(i) Continuous monitoring mechanisms are in place to detect discrepancies in real-time.

(ii) Any detected errors are flagged and escalated to the respective department for immediate resolution.

(iii) A post-correction review is carried out to ascertain the root cause and prevent recurrence.

(c) **Client Consent Management**:

(i) All activities that require Client consent are flagged in our systems.

(ii) Consent requests are sent to Clients via secure communication channels and are stored after acquisition.

(iii) Consent logs are maintained and reviewed periodically for compliance.

7.3 Withdrawal Process

(a) **Safe Plus Vault Withdrawals (Cold Wallet)**

(i) Service coverage: 24 hours Monday–Friday, and 09:00–00:00 HKT on Saturday, Sunday and Hong Kong public holidays.

(ii) Withdrawal processing time: within 4 hours Monday–Friday and within 9 hours on Saturday, Sunday and Hong Kong public holidays.

(iii) Workflow:

(1) The **Initiator** initiates the withdrawal via the Hex Trust platform.

(2) The Initiator confirms the withdrawal request using the **Hex Trust Mobile Application**.

(3) An **Approver** receives a notification on the Hex Trust Mobile App and may approve or reject the withdrawal request.

(4) A **Hex Trust operator** releases the funds from the Safe Plus vault.

(iv) Once the final step is completed, the request cannot be cancelled or reversed.

(b) **Safe Vault Withdrawals (e.g. Warm Wallet and Hot Wallet)**

(i) The Initiator initiates the withdrawal via the Hex Trust platform.

(ii) The Initiator confirms the withdrawal request using the Hex Trust Mobile Application.

(iii) Where the approval scheme is not set to 0-out-of-N, an Approver receives a notification on the Hex Trust Mobile App and may approve or reject the withdrawal request.

(iv) Upon satisfaction of the applicable enterprise approval quorum and policy engine criteria, Hex Trust automatically releases the funds from the Safe vault.

(c) For the avoidance of doubt, the detailed approval schemes and any limits governing withdrawals from each vault are as specified in the Custodian Handbook and may be updated by the Custodian with notice to the Company.

7.4 Reconciliation Procedures

(a) **Daily Reconciliation Process**:

(i) Every twenty-four (24) hours, an automated reconciliation process is initiated.

(ii) The process compares individual Client credit and debit ledger balances against the records in the VA wallets. Any mismatches trigger an automated alert for further review.

(b) These reconciliations include:

(i) **On-Chain Segregation**: Each Client's assets are stored in individually segregated wallets on-chain. Since each wallet is distinct and tied to a specific Client, the balances of these wallets can be easily verified by querying the blockchain.

(ii) **Automated Reconciliation Tools**: Hex Trust integrates automated tools to track transactions and balances in real-time. These tools compare on-chain data with the internal ledger, ensuring that all assets held within Hex Trust's custody match the blockchain records.

(iii) **API Integration**: Hex Trust's systems can be integrated with Clients' internal systems via APIs, allowing for continuous updates of balances and transaction history. This enables automated and real-time reconciliation of the assets without manual intervention.

(iv) **Auditing and Reporting**: Automated reports are generated regularly, comparing the on-chain balance of each Client's wallet with the internal record. Discrepancies, if any, are flagged and investigated promptly to ensure the integrity of the assets held in custody.

(v) **Discrepancy Reporting**: In the event of any material discrepancies during reconciliation that remain unresolved, we will promptly notify VARA in line with established protocols.

(c) **Reporting and VARA Communication**:

(i) Material discrepancies identified and not rectified within a stipulated period are compiled in a report.

(ii) The report is submitted to VARA following their specified reporting format and timelines.

7.5 Proof of Reserves

(a) **Maintenance and Review**:

(i) Reserve assets are reviewed on a daily basis to ensure they cover all Client VA liabilities.

(ii) The review process includes cross-verification with external statements and internal records.

(b) **Periodic Checks**:

(i) Quarterly checks are conducted to ensure alignment with VARA's evolving requirements related to reserve assets.

(ii) These checks involve both quantitative analysis and qualitative assessments.

(c) Approach and Methodology:

(i) **Asset Balance Verification** - Verifying the cryptocurrency holdings as reported by the VASP.

(a) Obtain the asset balance report generated from the platform, listing the quantity and type of cryptocurrencies held in different wallets or exchanges as of the reporting date. Ensure the report includes the nominal value of each cryptocurrency based on the market price at the specified date. Compare the balance report with third-party custodial accounts to verify the existence and ownership of assets.

(ii) **Crypto Holdings Reconciliation** - Ensuring consistency between platform records and third-party wallet/exchange statements

(a) Obtain wallet and exchange statements from third- party custodians and reconcile the quantity of cryptocurrencies held as per the statements with those reported in the asset balance report.

(iii) **Reconciliation with Financial Records** - Confirming that the reported wallet and exchange balances are accurately reflected in the Company’s financial records

(a) Obtain the trial balance as of the reporting date and compare the wallet and exchange balances recorded in the Company’s books of accounts with the balances in the wallet/exchange statements.

(iv) **Users Crypto Balances** - Validating the cryptocurrency balances attributed to individual Users

(a) Obtain a customer-wise cryptocurrency balance report detailing user IDs, the number of coins held by each customer, and their value as of the reporting date. Verify the accuracy and completeness of the report, ensuring that no discrepancies exist between internal customer records and platform balances.

(v) **Customer Liability Report Reconciliation** - Ensuring that customer liabilities are properly reflected in the VASP's financial records

(a) Obtain the customer liability report from the platform as of the reporting date and compare it with the customer-wise cryptocurrency balance report.

(b) Ensure that all customer holdings are fully represented in the platform's liability records.

(vi) **Financial Reconciliation of Customer Liabilities** - Confirming the accuracy of customer liabilities recorded in the Company's financial statements

(a) Compare the customer liability amounts recorded in the Company's books as of the reporting date with the liabilities reported on the customer liability report generated by the platform.

(vii) **Wallet Storage Structure** - Validating the segregation of assets held in Hot, Warm, and Cold storage wallets

(a) Obtain detailed records of assets stored in Hot, Warm, and Cold wallets, verifying balances and wallet addresses as of the reporting date.

(viii) **Net Asset/Liability Calculation by Asset Class** - Calculating the net assets or liabilities by asset class to verify whether the Company's reserves adequately cover its liabilities

(a) Compare the value of each asset class in the asset balance reports with the customer liability report generated from the platform and calculate the net position (assets minus liabilities) by asset class.

(ix) **Reconciliation of Crypto Assets with Liabilities** - Ensuring that the Company's cryptocurrency reserves fully cover customer crypto liabilities

(a) Compare the total cryptocurrency assets with the customer crypto liabilities recorded in the Company's books as of the reporting date, calculating the net position (net assets or liabilities).

7.6 **Training and Competency**

(a) Employee Training Modules:

(i) A specialized training curriculum is in place for employees directly handling Client VAs.

(ii) This curriculum covers regulatory requirements, our internal procedures, and best practices in asset management.

(iii) Employees undergo this training upon induction and are required to attend

refresher courses annually.

7.7 **Trading, Trading Vaults, and Settlement**

(a) **Trading Access:** Only users assigned the Trader role by the Company (and recorded in the Custodian Handbook) may execute trades via the Hex Trust trading interface. Users assigned the Trade Viewer role have view-only access to trading and settlement information.

(b) **Trading Vaults and Trading Accounts:** The Company may maintain one or more Trading Vaults, each of which may contain one or more Trading Accounts dedicated to holding assets used exclusively for trading. Each Trading Account has a unique deposit address to enable precise allocation and tracking of assets used for trading.

(c) **Settlement and Cut-Off Time:** Settlement refers to the final transfer of bought and sold assets between parties following execution of a trade. Hex Trust provides secure settlement services for all trades conducted via its platform. The daily settlement cut-off time is 14:00 (UTC+8). Any ad-hoc settlement requirements outside of standard cut-off may be requested via the Hex Trust support channels.

(d) **Gas Station Vault:** To prevent transaction failures due to insufficient gas, the Company may maintain a Gas Station vault with the Custodian. This vault is used to automatically fund network gas fees for settlements originating from the Company's Trading Vaults in line with the Custodian Handbook.

8. COMPANY CUSTODY ARRANGEMENT

8.1 The Virtual Assets shall be held by the Custodian, which shall be responsible for their safekeeping, as custodian, for the account of the Client on and subject to the terms of this Agreement. The Company has agreed not to pledge, charge, grant an option or otherwise create any encumbrances on the Virtual Assets without the prior written consent of the Custodian.

8.2 The Company has confirmed, acknowledged and consented that the Custodian is authorized, to the extent it is in compliance with the applicable law (including but not limited to legislations regarding anti-money laundering crimes and combating the financing of terrorism and financing of illegal organizations in the UAE) and VARA's requirements, to appoint, as the Custodian deems appropriate, any agents or sub custodians, whether in its own name or that of the Company, to perform any of the duties of the Custodian under the custody agreement and is entitled to deposit the Virtual Assets in or with any depository system of its preference.

8.3 The duties of the Custodian shall include:

(a) to hold the Virtual Assets in separate accounts in its books, to arrange for the Virtual Assets to be deposited in the Wallet or otherwise held by or to its order as it may think proper for the purposes of providing for their safekeeping, and to record the amounts and locations thereof;

(b) to provide periodical reports substantiated for the decision-making; and

(c) The Custodian shall not: (i) use or commingle the Virtual Assets with its own funds or with those of any other customers; (ii) make any loans using the Virtual Assets as collateral or security; or (iii) take any action that would cause the Virtual Assets to be used for any purpose other than as instructed pursuant to an Instruction of the Company.

8.4 The duties of the Client shall include:

(a) Provide timely the List of Authorised Users, the List of Authorised Signatories and the List of Authorised Account Admins to be included in the Handbook as per Clause 4.1 or in Schedule C (as the case may be) inline the custody agreement;

(b) provide timely changes to any information and the Company authorisations required, necessary, or appropriate in connection with this Agreement in writing or in such manner as may be reasonably required by Custodian or as required by any applicable law, VARA's requirements or any other international regulatory requirements;

(c) provide to Custodian any documents that may reasonably be requested by the Custodian for the purpose of the KYC and AML procedures and any information as may be reasonably required by the Custodian or as required by any applicable law, VARA's requirements or any other international regulatory requirements in relation to the origin of the Virtual Assets deposited or expected to be credited to the custody of Hex Trust;

(d) provide to Custodian all information that may reasonably be requested by the Custodian for the purpose of complying with Travel Rule, including without limitation name, residential address and wallet address of the originator and beneficiary of certain Virtual Assets' transactions, a list of the Client's most-frequently used (also known as whitelisting of) wallet addresses to facilitate the Custodian's compliance with Travel Rule; and

(e) provide all reasonable assistance to the Custodian for complying or fulfilling any requests, enquiries or requirements from relevant government authorities and/or regulatory organization(s) (including but not limited to VARA). For the avoidance of doubts, the Custodian shall have the rights (and be deemed to have the Company authorisation) to provide any information or documents received from the Company in relation to the custody agreement to the relevant government authorities and/or regulatory organization(s) pursuant to their requests, enquiries or requirements.

8.5 The services provided to the Company by the Custodian under custody agreement shall be deemed non-exclusive, and nothing contained in or implied by this agreement shall be construed so as (i) to prevent the Custodian, its agents or its or their associated companies, principals, affiliates or employees in any way from purchasing, selling or otherwise dealing in any VAs or other assets (whether forming part of the VA or not) for its or their own account prior to, simultaneously with, or subsequent to any dealings on behalf of the Company, or (ii) from providing similar services to or entering into similar agreements with any customers or other persons or (iii) to impose any duty of disclosure or liability to account for any profit made by any of them in relation to any of the foregoing.

8.6 Under our custody agreement with Hex Trust, the Company's designated officers, employees, or agents select the wallet type at the time of deposit. Hex Trust, as the custodian, is responsible for ensuring the safekeeping of VAs in line with security protocols and operational requirements.

8.7 OTC Trades and Settlement from Custody

(a) OTC trades executed by the Company's authorised persons under any Master Trading Agreement entered into with Hex Trust or its designated trading entity may be settled directly from the Company's Hex Safe account(s).

(b) For this purpose, the relevant OTC trade order and related confirmations shall be treated as an "Instruction" under the custody agreement and the Custodian Handbook, and the Custodian is entitled to rely on such Instruction without liability on its part, subject to the applicable disclaimers and terms and conditions in the custody documentation.

8.8 Security Controls for Custody Access

(a) Account Credential and First-Time Login: Each Authorised User receives a first-time login email from the Custodian to set up their account, including a strong password and initial access credentials.

(b) Two-Factor Authentication (2FA): Upon first login, users are required to enable 2FA (currently via Google Authenticator) as a mandatory control. Access to custody functions without 2FA is not permitted.

(c) Hex Trust Mobile Application: The Hex Trust Mobile App is used as an additional security factor for authorising initiations and approvals of transactions. Initiators and Approvers must confirm instructions through the mobile app in accordance with the Custodian Handbook.

(d) Custodian Verification Rights: Hex Trust reserves the right to perform additional identity or credential verification at any time (including random checks) in line with its security protocols and the Custodian Handbook.

8.9 Bankruptcy Remoteness of Client Assets

(a) Segregation of Assets: The Policy mandates the segregation of Client assets from the Custodian's own assets. This segregation is crucial to ensure that client assets are not affected by the Custodian's financial status. Clause 06, Duties of Custodian of our custody agreement explicitly states that client assets will be held in separate accounts, distinctly identified and maintained independently from the Custodian's assets. As such, all Client assets are recorded in separate ledgers and wallets, with detailed documentation to prevent any commingling with the Custodian's funds.

(b) Regular Audits and Compliance Checks: Our policies mandates regular internal and external audits to verify the proper segregation and protection of client assets. Provisions within the custody agreement grant clients the right to request audit reports and compliance confirmations regarding the status and safekeeping of their

assets. These audits ensure that the Custodian adheres to all policies related to asset segregation and bankruptcy remoteness, with findings reported to both internal governance bodies and clients.

(c) Transparency and Client Communication: Our policies ensure that clients are regularly informed about the measures in place to protect their assets, including their bankruptcy remote status. The agreement includes clauses that require the Custodian to provide clear and timely updates on any changes to the legal or operational framework that might impact the status of client assets. Regular reports and communications are sent to clients detailing the safeguarding measures and confirming the bankruptcy remote status of their assets.

9. REPORTING BREACHES AND DISCREPANCIES

9.1 Internal Reporting:

(a) **Identification**: Any employee who identifies a potential breach or discrepancy is obligated to report it immediately through our internal reporting system.

(b) **Preliminary Assessment**: Once a potential issue is reported, a dedicated team will perform a preliminary assessment to determine the severity and potential implications.

(c) **Escalation**: Material breaches or discrepancies will be escalated to senior management and the compliance department for immediate action.

9.2 Reporting to VARA:

(a) **Documentation**: All relevant details of the identified breach or discrepancy will be documented in the format stipulated by VARA.

(b) **Notification**: VARA will be notified immediately for material breaches or discrepancies that cannot be rectified within a specified timeframe.

(c) **Continuous Communication**: Our Company commits to maintaining open communication with VARA, updating them on the status of the breach's resolution and any measures taken to prevent its recurrence.

10. REVIEW OF POLICY

10.1 Periodic Reviews:

(a) **Frequency**: This policy will be reviewed annually to ensure it remains aligned with regulatory requirements, industry best practices, and our Company's operational dynamics.

(b) **Feedback Mechanism**: All departments handling Client VAs are encouraged to provide feedback during these reviews, suggesting areas of improvement or potential risks.

(c) **Documentation**: Each review's findings and subsequent updates to the policy will be documented and archived for future reference and audit purposes.

10.2 Triggered Reviews:

(a) **Basis**: Apart from the scheduled annual reviews, this policy will undergo an immediate review in the event of significant regulatory changes, material breaches, or systemic failures.

(b) **Implementation**: Recommendations from triggered reviews will be implemented immediately upon validation, and relevant stakeholders will be notified.

Annexure 01
Responsibilities for Client VA Movement Based on Roles

Auditor:

View Account: Auditors can view account balances and activity logs related to client VAs. They do not have permission to initiate or approve transactions but can review all actions for compliance purposes.

Initiator:

View Account: Initiators can view the account details, including balances and transaction history.

Initiate Deposit/Withdrawal: Initiators are responsible for starting the process of depositing or withdrawing client VAs. They will request VA movements, which then need approval before being executed.

Approver:

View Account: Approvers have access to view account information.

Approve Withdrawal: Approvers are responsible for reviewing and approving withdrawal requests initiated by the Initiator. This role ensures that any VA movement is properly authorized and compliant with internal controls and regulations.

Hex Trust Operator (Custodian Role):

This is an operational role performed by Hex Trust personnel, not by the Company. For Safe Plus vault withdrawals, once all Initiator and Approver actions are completed, a Hex Trust operator releases the funds from the vault in accordance with the Custodian Handbook.

Account Admin:

Manages user roles, vaults, address books, address whitelists, and related enterprise configuration within the Hex Trust platform. Cannot initiate or approve withdrawals unless also assigned Initiator/Approver roles.

Admin Approver:

Approves changes to address books, whitelists, transaction policies, withdrawal limits and other enterprise-level settings as defined in the Custodian Handbook. Required

sign-off for key enterprise configuration changes and 2FA reset requests.

Trader:

May execute trades in Trading Vaults / Trading Accounts. Can view trade, settlement and order history but cannot initiate or approve withdrawals from Trading Vaults unless also assigned Initiator/Approver roles.

Trade Viewer:

View-only access to trading and settlement data in Trading Vaults / Trading Accounts. Cannot initiate, approve or execute any transactions.

Based on the aforementioned roles, the compliance function and Compliance Officer will be explicitly involved in the Approver role (and, where appropriate, in Admin Approver and Account Admin roles), particularly in relation to transactions that trigger alerts or freezes due to predefined rules on Chainalysis or due to transaction limits configured within the Hex Trust platform.