Stake RWA FZE Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Policy ("AML/CFT Policy")

Document Control

Document Control	
Document Name	Stake RWA FZE
Document Owner	Compliance Officer and Money Laundering Reporting Officer
Document ID	TBD
Classification	Internal
Version Number	1
Status	First issuance
Publish Date	TBD
Revision Date	Legislative/business changes or 1 year, whichever comes earlier 1 year from publish date

Document Amendment Control			
Version	Date	Change Description	Update By
1	TBD	New handbook/first issuance	

Table of Contents

Terms of Reference

ML	Money Laundering
TF	Terrorist Financing
AML/CFT	Anti-Money Laundering and Counter Terrorism Financing
FIU	Financial Intelligence Unit
KYC	Know Your Customer
KYT	Know Your Transaction
PEP	Politically Exposed Person
UBO	Ultimate Beneficial Owner
FATF	Financial Action Task Force
EOCN	UAE Executive Office for Control & Non-Proliferation
OFAC	Office of Foreign Assets Control
MLRO	Money Laundering Reporting Officer
CDD	Customer Due Diligence
EDD	Enhanced Due Diligence
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
SOF	Source of Funds
i-STR	Internal Suspicious Transaction Report or Activity Report
E-STR	External Suspicious Transaction Report
VARA	Dubai Virtual Assets Regulatory Authority.
UAE	United Arab Emirates
CMS	Compliance Management System

1. Definitions

- Customer: Means any legal person who attained the age of 18 with legal capacity who successfully creates an account in Stake RWA FZE and successfully completed and passed their Know You Customer ("KYC").
- Prospective Customer: Means any legal person who has attained the age of 18 with legal capacity who has not created an account in Stake RWA FZE nor passed their Know You Customer ("KYC") yet.
- Onboarding Process: Customer onboarding is the procedure through which a business or organization brings in and integrates new Customers into their systems, products, or services. This includes gathering essential information, verifying and identifying Customer, and completing necessary documentation or agreements to establish a formal business relationship with the Customer.
- GoAML: means the electronic platform through which Suspicious Transaction reports can be submitted to the UAE FIU.
- Compliance Officer: As defined in VARA Compliance and Risk Assessment Rulebooks. Throughout this policy, the term 'Compliance Officer' refers to the individual holding the roles of both Compliance Officer and MLRO.
- MLRO: As defined in VARA Compliance and Risk Assessment Rulebooks. Throughout this policy, the term "MLRO" refers to the individual holding the roles of both Compliance Officer and MLRO.
- Virtual Asset: A digital representation of value that may be digitally traded, transferred, or used as an exchange or payment tool, or for investment purposes. This includes Virtual Tokens, and any digital representation of any other value as determined by VARA.
- Employees: Means all individuals working for Stake RWA FZE including the members of the Senior Management but excluding members of the Board. If an individual is both a member of the Senior Management and a member of the Board, then such individual is also considered as Employees.
- Sanctions: Restrictions imposed by governments or international bodies on individuals, entities, or countries due to suspected involvement in unlawful or prohibited activities.
- Adverse Media: Refers to negative information from various sources that indicates potential involvement in illicit or high-risk activities.

- Face Match: An advanced detection technology designed for performing the facial biometric check between Customer's selfie and identification document provided. The neural network scans a face and creates a 3D map for analysing the image and adapting to its changes.
- Suspicious Activity: means transactions, attempted transactions, or funds which a Company has reasonable grounds to suspect as constituting, in whole or in part, and regardless of the amount or the timing, any of the following—

- the proceeds of crime [whether designated as a misdemeanour or felony, and whether committed within the Emirate or in another country in which it is also a crime];
- being related to the crimes of money laundering, the financing of terrorism, or the financing of illegal organisations; and
- being intended to be used in an activity related to such crimes.

- Regulatory Authority: Refers to a government agency or body responsible for creating, implementing, and enforcing rules and regulations within a specific industry or sector, guiding compliance efforts in AML policies, and necessitating obligatory reporting by companies under its jurisdiction.
- Red Flags: Indicators, often derived from patterns or anomalies in financial transactions or Customer behaviour, that suggest a heightened risk of money laundering, fraud, or other illicit activities, prompting closer scrutiny and potential reporting as part of AML policies.
- Retail Investor: As defined by VARA Market Conduct Rulebook.
- Board: Means the board of directors of the Company.

2. Introduction

2.1 Purpose of the Policy

Stake RWA FZE (the "Company") has developed and implemented this Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Policy (hereinafter referred to as the "Policy") to outline the procedures and guidelines that must be strictly followed in compliance with the Virtual Asset Regulatory Authority of UAE (VARA) Broker Dealer Rulebook, as well as other applicable laws and regulations related to AML/CFT.

The Company is committed to strictly prohibiting and actively preventing Money Laundering (ML) and Financing of terrorism (FT), or support for illegal organizations and criminal activities. This commitment is upheld via full compliance with all applicable requirements under UAE AML/CFT laws and their implementing regulations.

The Company shall operate as a Broker Dealer, regulated under the laws and regulations of VARA. The Company commits to all responsibilities and conditions imposed by the Policy with utmost seriousness and to that end; all Employees are required to review and abide by the content of this Policy and comply with all of its requirements.

2.2 Regulatory Context

The Company has developed and implemented this Policy based on a thorough self-assessment of the inherent ML and TF risks associated with its business activities. This Policy has been prepared in accordance with:

- VARA Broker Dealer Rulebook;
- VARA Compliance and Risk Management Rulebook;
- VARA Compulsory Rulebooks;
- The Federal AML-CFT Laws;
- The Financial Action Task Force's [FATF] 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers [June 2020];
- FATF's Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers [July 2021];
- FATF's Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [October 2021];
- The International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations [March 2022];
- Cabinet Resolution No. [74] of 2020 regarding the Terrorist List System and The Implementation of Security Council Resolutions Related to Preventing and Suppressing Terrorism and its Financing, Counter of Proliferation and its Financing, and the Relevant Resolutions;
- The UAE Executive Office for Control & Non-Proliferation [EOCN] Guidance on Counter Proliferation Financing for FI's, DNFPBs, and VASPs [March 2022];
- The MENA (Middle East and North Africa) Financial Action Task Force (MENA FATF) regulations;
- Directives issued in the UAE for implementation of the United Nations Security Council Resolutions (UNSC) relating to the suppression and combating of terrorism, terrorist financing and proliferation of weapons of mass destruction and its financing; and

- Adoption of Sanction and screening Lists:
    - European Union Sanctions (EU)
    - United Nations Sanctions (UNSC)
    - The Office of the Foreign Assets Control (OFAC)
    - Her Majesty's Treasury (HMT)
    - Monetary Authority of Singapore (MAS)
    - FATF watchlist
    - The UAE's local Terrorist List, as may be amended from time to time.

2.3 International Bodies

The policy also refers to international bodies, regulations, and industry standards on AML/CFT including but not limited to:

- Resolutions and sanctions issued by the UN Security Council and other bodies;
- Recommendations of the Financial Action Task Force ("FATF");
- Recommendations of the Middle East & North Africa Financial Action Task Force (MENAFATF);
- Financial Crimes Enforcement Network (FinCEN);
- Office of Foreign Assets Control (OFAC);
- European Union (EU).

2.4 Scope of Policy

This Policy serves as a comprehensive guide for the Board, Senior Management, and Employees of the Company, detailing their responsibilities in preventing ML and FT. All Employees, including senior management, are required to thoroughly read, understand, and adhere to this Policy.

2.5 Ownership & Governance

The Compliance Officer, who will also act as the MLRO at the same time (The individual handling both roles shall be herein referred as "MLRO") is responsible for the development, implementation, and oversight of this Policy and must ensure this Policy is duly approved by the Board. Following the approval of the Board and MLRO will ensure this Policy is available to all of the Employees at all times.

2.6 Policy Review & Updates

This Policy is subject to periodic review by the MLRO to ensure it remains up-to-date with legal and regulatory developments, on a yearly basis or sooner if a material change has occurred. Any necessary amendments will be made and approved in accordance with the Company's internal governance procedures.

The provisions of this Policy, along with any subsequent revisions, will become effective immediately upon approval by the Board.

The proposal for a review and the review of this Policy may be scheduled more often, including but not limited to the following material changes:

- Change of Company structure and operations;
- Changes to the governing laws and regulations;
- Changes in the business or Customer base;
- Changes in risk profile of the Company;
- Unaccounted Incident of Suspicious Activity.

This Policy shall be accepted and approved by the Board of Directors. This Policy must be followed by all Employees of the Company.

The MLRO of the Company must ensure that all Employees of the Company (including the full-time Employees, part-time Employees, newly recruited, outsourced functions, if any, and directors) are made aware of this Policy in writing.

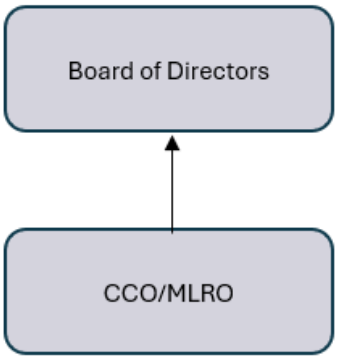
2.7 Risk Appetite Statement

The Company accepts low risk in the areas of AML, Sanctions Compliance, and Anti-Bribery, Corruption, Proliferation Financing, and Counter-Terrorism Financing recognising that these risks, if unmanaged, could expose the Company to significant regulatory, financial, and reputational damage. In line with the Company's growth strategy, we will take a measured and proactive approach to mitigate these risks while ensuring compliance with all applicable laws and regulations.

3. Governance of the AML/CFT Program

3.1 Governance Structure

The Governance of a Company broadly refers to mechanisms and processes by which the Company is managed, controlled, and directed. The Governance structures and principles have been identified and the distribution of powers and responsibilities within the management structure of the Company has been comprehensively provided below for ease of understanding.



3.2 Duties and Responsibilities

a. Board of Directors:

The Board must assume responsibility and exercise due skill, care and diligence for all responsibilities stated in the "Detailed Roles and Responsibilities" document properly record kept by the Company.

b. Senior Management:

Executing and monitoring the Company's AML/CFT framework. This position is central to fostering a strong culture of compliance and ensuring that the Company's operations remain in line with applicable regulatory standards.

c. Compliance Officer & MLRO:

The Company's full time Compliance Officer who will also act as a MLRO at the same time and will be responsible to ensure the below:

- Developing and implementing compliance and AML/CFT policies and procedures;
- Ensuring that all Employees, including Senior Management and Board of Directors, are properly and adequately trained in order to understand and comply with all applicable laws, regulatory requirements and AML/CFT Laws particular those relevant to Virtual Asset Activities;
- Assessing emerging issues and risks relating to the Company's activities and ML/TF trends;

- Conducting AML/CFT risk assessments in accordance with VARA's Compliance and Risk Management Rulebook and implementing all necessary changes to the Company's relevant policies and procedures to address such issues and risks;
- Reporting compliance activities, compliance audits, and reports to the Board;
- Assuring that appropriate corrective actions are taken in response to inadequacies in the Compliance function/or noncompliance with any applicable laws, regulatory requirements and any Federal AML/CFT laws, if necessary.
- Monitoring and reporting Suspicious Transactions in accordance with VARA Compliance and Risk Management Rulebook;
- Implementing all relevant AML/CFT policies and procedures and shall remain accountable for all associated obligations.
- Monitoring all Customers, transactions, and alerts generated by the AML/KYC system and the Transaction Monitoring System;
- Engaging proactively in both internal and external AML/CFT audits and regulatory inspections;
- Managing any outsourcing arrangements related to AML/CFT functions and ensuring that such arrangements are properly monitored and remain compliant with VARA Company Rulebook.
- Organize AML/CFT training appropriate to the Company's business model and Employees' responsibilities, and regularly assess the effectiveness of the training programs.
- Ensure that all documentation relating to Customers, transaction flows through the company's systems, internal compliance activities, training, and suspicious transaction reports (STRs) are retained for a minimum of eight (8) years.
- Acting as focal or pivotal point of contact between the FIU, the Regulator(s), and State authorities in relation to AML issues.

In addition to the above, the MLRO shall report directly to the Board on all aspects of the AML/CFT policies and procedures within the Company, including:

- Reporting to the Board on a quarterly basis on the effectiveness of the Company's AML/CFT policies and procedures, identifying any failures in such policies and procedures and/or any non-compliance with any Federal AML/CFT Laws. This report includes an

analysis of operational and compliance indicators such as the number of applications received and customers successfully onboarded, along with the reasons for any rejected Potential Customers. The review also accounts for the number of Customer relationships that were terminated, including justifications for such decisions. Furthermore, transaction volumes, both processed and rejected for compliance reasons, must be reviewed. The MLRO should evaluate the training activities conducted during the period, note any amendments made to internal policies and procedures, and consider the impact of any new legislation or emerging AML/CFT risks.

- Reporting to the Board and VARA on Annual basis a holistic evaluation of the company's AML/CFT compliance programme. The report should provide a summary of significant developments and areas of concern noted over the reported year. It must highlight regulatory updates and summarize the Company's AML/CFT performance. Any revisions to internal AML/CFT policies should be documented along with the rationale behind these changes. The report should also cover a comprehensive risk assessment and provide details of AML/CFT Employees' training activities. The MLRO must also include details on any STR/SARs filed, any AML/CFT incidents or breaches identified during the year, their consequences, and the measures taken in response. Lastly, the report should discuss notable regulatory developments, any formal engagement with supervisory authorities, outcomes of audits, and strategic plans for the upcoming year.
- Making the reports required under VARA Compliance and Risk Management Rulebook available to VARA on request;
- Escalate compliance activities, inefficiencies, compliance audits, and reports to the Board.

The Company ensures that the MLRO is, at all times, a fit and proper person, is employed on a full-time basis by the Company, is resident in the UAE, and possesses relevant experience appropriate to the nature, scale, and complexity of the Company's activities. The MLRO shall have unrestricted access to all necessary information and resources and shall report directly to the Board.

a. Compliance Reviews

On a quarterly basis, the MLRO is responsible for conducting a comprehensive review to evaluate the company's adherence to its internal AML/CFT policies and procedures. This review includes an analysis of operational and compliance indicators such as the number of applications received and

customers successfully onboarded, along with the reasons for any declined applications. The review also accounts for the number of customer relationships that were terminated, including justifications for such decisions. The MLRO must also oversee a quarterly screening of the entire customer base against sanctions lists, legal prosecutions, and negative media sources. Furthermore, transaction volumes, both processed and rejected for compliance reasons, must be reviewed. The MLRO should evaluate the training activities conducted during the period, note any amendments made to internal policies and procedures, and consider the impact of any new legislation or emerging AML/CFT risks. Following this assessment, a summary of the findings must be formally presented to the Board.

d. Internal Audit Department

The Internal Audit Department serves as the third line of defence within the Company's AML/CFT compliance framework. This function operates independently from the operational functions and reports regularly and directly to Senior Management. It conducts periodic assessments of the effectiveness of the Company's internal compliance program within its regulated scope.

To support management in fulfilling its responsibilities, the Internal Audit Department reviews internal processes and control systems, identifies areas for improvement, and monitors the implementation of corrective actions. The key focus areas of Internal Audit activities include:

- Review the adequacy and effectiveness of AML/CFT policies, procedures, and internal controls applicable to the Company's own activities.
- Evaluate the performance and efficiency of the Company's Compliance function in meeting its regulatory obligations.
- Person audit work on a regular basis;
- Inform Senior Management of findings and recommendations;
- Conduct follow-up audits to verify the timely and adequate implementation of corrective measures.
- Gather sufficient and appropriate audit evidence to support conclusions and recommendations, and to meet the expectations of external and regulatory auditors with respect to the Company's AML/CFT obligations.

e. The Employees

All Employees are responsible for adhering to applicable AML laws and this Policy. They must attend all AML/CFT training sessions organized by the Company. Additionally, Employees are required to promptly report any Suspicious Activities to the MLRO via i-STR/i-SAR, refrain from any form of tipping off the Customer, and uphold strict confidentiality regarding Customer information and any AML/CFT-related matters.

The Company shall establish and maintain procedures to ensure that only qualified individuals with the appropriate skills, knowledge, and experience are employed. The Company maintains sufficient employment levels to effectively perform all relevant duties. The Company ensures all Employees receive timely and up-to-date information on the Company's policies and procedures. Adequate training relevant to each Employee's role shall be provided upon hiring and continuously thereafter. In addition to regular AML/CFT training with ongoing monitoring of Employee's compliance.

All operational policies, procedures, and compliance policies must be communicated to new Employees within their first thirty (30) calendar days. When any policies or procedures are updated, the Company shall notify all relevant Employees and ensure that the most current versions are readily accessible at all times.

4. Financial Crimes and AML/CFT Framework

The Company is committed to identifying, assessing, and mitigating the risks of Money Laundering, Terrorist financing, Proliferation Financing, and international sanctions through effective Customer Due Diligence (CDD), ongoing monitoring, and prompt reporting of suspicious activity, in line with applicable laws and regulatory requirements.

4.1 Money Laundering (ML)

Any person who commits intentionally one of the following actions, with the knowledge that the assets are acquired from an offence or felony, shall be considered to have committed a crime of ML:

- Converts, transfers, deposits, saves, invests, exchanges or manages any proceeds, with intent to conceal or disguise the illicit origin thereof;
- Conceals or disguises the true nature, origin, location, way of disposition, movement, rights related to any proceeds or the ownership thereof; or
- Acquires, possesses or uses such proceeds.

- Any attempt to ML is also a criminal offence.

Any of the following acts shall be deemed to be an act of participation in the offence of ML:

- Destruction, misappropriation, concealment and/or forgery of any document which could be used as evidence in the offence or against the accused;
- Knowledge of the intent of any individual involved in the offence and provision of any facilities or information which may assist such individuals to conceal the offence or escape from prosecution.

a. Stages of Money Laundering:

- Placement stage: the stage where illegal funds enter the financial system. This commonly involves paying cash into a bank account, making a money remittance, deposit bearer values;
- Layering stage: the second stage is concerned with transferring and transforming funds and assets from one account into the other, one bank to another, one jurisdiction to another, so that they cannot easily be traced back to their source. These are often complex financial transactions aimed at disguising the audit trail and providing anonymity for the criminal;
- Integration stage: in the final stage, the funds are brought back into circulation in clean and usable form or are transformed into clean assets (for instance by purchasing and selling financial instruments or real estate, early reimbursement of mortgages and loans, etc.).

4.2 Terrorist Financing (TF)

TF is defined as the provision or facilitation of funds (legitimately or illegitimately) for the purpose of sponsoring terrorist activity. It may involve funds raised from legitimate sources such as personal donations, profits from businesses, and charitable organizations, as well as funds raised from criminal sources such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping, and extortion. This is one of the most significant threats that all financial institutions around the world are facing. The terrorism financing process generally involves:

- Raising funds through donations, self-funding, microloans, or criminal activities.
- Making a financial transfer to a terrorist, terrorist network, terrorist organization, or terrorist cell.
- The funds could be used for a variety of purposes, such as purchasing weapons or bombs, making payments to terrorists or insurgents, or funding the expenses of terrorist organizations.

4.3 Proliferation Financing

Proliferation financing is the act of providing funds, assets, or other economic resources, directly or indirectly, to individuals, entities, or groups for the development, acquisition, manufacture, possession, transfer, or use of weapons of mass destruction, including nuclear, chemical, or biological weapons, and their means of delivery, as well as related materials and dual-use technologies. This includes any activity that facilitates the evasion, breach, or non-implementation of targeted financial sanctions issued pursuant to United Nations Security Council resolutions.

4.4 International Sanctions

International Sanctions are punitive or coercive measures against a country, regime, entities or individuals. International Sanctions typically include:

- Country or regime Sanctions which are applied against a country, including its nationals, or government regime;
- List based Sanctions which are targeted against specific individuals, or entities or vessels;
- Sanctions are used to place restrictions on the activities of a country or specific individual or groups.

Punitive or coercive measures may include:

- Restrictions on trade in goods or services;
- Restrictions on financial transactions, investment restriction or asset freezes;
- Restrictions on exports and/or imports or trade embargoes;
- Military Sanctions (Arm Embargoes, No-Fly Zones, and Military Interventions);

- Diplomatic Sanctions (Diplomatic Isolation, Suspension of Diplomatic Relations and Expulsion of Diplomats);
- Travel bans or visa restrictions; or
- Participation bans.

5. Compliance Management System

The Compliance Management System ("CMS") plays a pivotal role in the Company's commitment to maintaining robust AML and CFT practices. It serves as a framework for effective risk management, regulatory compliance, and internal governance. The CMS is designed to detect, prevent, and address potential compliance violations and to ensure the Company operates in full adherence to all applicable laws, regulations, and internal policies at all times.

The CMS shall be overseen by the MLRO, who is responsible for establishing and maintaining the CMS. The MLRO operates independently from the Company's business and operational functions and reports to the Board. In cases of material non-compliance by the Company, its Board, or Employees, the MLRO is responsible for notifying VARA and any other relevant authorities without delay.

The Company will undergo risk-based compliance testing and monitoring programme designed to regularly review different areas of the business, identify key risk indicators, and evaluate performance.

The Board and all Company Employees shall have full access to compliance records, documentation, policies, and information required for effective oversight.

The CMS comprises the following core elements:

- Compliance Policies and Procedures: Clear, detailed, and enforceable procedures covering AML/CFT obligations, licensing conditions, record-keeping, Customer and proprietary dealings, and Employee conduct.
- Responsible Individuals: The MLRO is responsible for establishing and administrating the CMS.

- Risk Assessment and Monitoring: A risk-based compliance testing and monitoring procedures designed to regularly review different areas of the business, identify key risk indicators, and evaluate performance.
- Reporting and Escalation: Mechanisms to report compliance breaches and escalate material issues in a timely manner to the CO and, where required, to regulators.
- Training and Awareness: Ongoing training programmes to ensure all Employees understand their compliance obligations and are equipped with the knowledge and tools to fulfil them.
- Customer Lifecycle Compliance: Technical and procedural safeguards to ensure compliance in areas such as customer onboarding, transaction monitoring, the Travel Rule, and enhanced due diligence.

The CMS covers compliance policies and procedures, risk assessment, monitoring, reporting, training and awareness. Throughout this Policy and the following sections, the Company emphasizes technical expertise and risk-based competence in areas like customer onboarding, transaction monitoring, and travel rule.
The subsequent sections ensure full adherence to legal and regulatory requirements, along with periodic reviews and updates of compliance policies.

6. Risk Based Approach

The Company shall take the appropriate and diligent steps to identify and assess any ML and TF risks to which its business is or may potentially be exposed to, considering the nature, size and complexity of the Customer's profiles and activities.
The Company acknowledges and adopts *FATF's Updated Guidance for a Risk Based Approach for Virtual Assets and Virtual Asset Service Providers*, to ensure that the Company implements the appropriate processes by which the MLRO allocates its resources in areas of high risk or areas in which they should prioritize allocation of resources and adopts risk-appropriate tools to achieve effective and efficient AML/CFT supervision and mitigate any direct and indirect AML/CFT risks.

The Company assesses and addresses its ML risks by reviewing the risks to which it is exposed to (Customer risk, geographical risk, product & service risk, relationship risk, new technology/delivery method risk, internal framework risk) as a result of the nature of its business, Customers, products,

services and any other matters which are relevant in the context of ML and then adopting a proportionate approach to mitigate those risks;

All risk-based assessments undertaken for the purposes of complying with the AML/CFT Policy shall be:

- Objective and proportionate to the risks;
- Based on reasonable grounds;
- Properly documented; and
- Updated at appropriate intervals.

The Company is committed to:

a. Taking appropriate steps to identify and assess ML risks to which its business is exposed to, taking into consideration the nature, size and complexity of its activities;

b. Identifying and assessing the risks taking into account:

- Type of Customers and their activities;
- Countries or geographic areas in which it operates;
- Products, services and activity profiles;
- Complexity and volume of transactions;
- Type of Virtual Assets;
- Distribution channels and business partners;
- Development of new products and new business practices, including new delivery mechanisms, channels and partners; and
- Use of new or developing technologies for both new and pre-existing products.

c. Taking appropriate measures to ensure that any risk identified as part of the assessment is taken into account in its day-to-day operations, including:

- Development of new products/services, business practices & technologies;
- Taking on of new Customers; and
- Changes to its business profile.

d. Undertaking AML Business Risk Assessment with respect to the following:

- Development and maintenance of the Company's AML policies, procedures, systems and controls;
- Ensuring that the Company's AML policies, procedures, systems and controls adequately mitigate the identified risks;
- Assessment of the effectiveness of its AML policies, procedures, systems and controls;
- Assisting in allocation and prioritisation of AML resources; and
- Assisting in the carrying out of the Customer risk assessment.
- Assessment of the Anonymous-Enhanced Virtual Assets: The only tokens the Company deals with are real estate–issued tokens, which are issued and transacted on transparent blockchains. This ensures that key transaction details, such as the wallet addresses and transaction amounts, are publicly visible and traceable. All transactions are subject to monitoring, screening, and risk scoring by the Company's Transaction Monitoring Service Provider. The MLRO is responsible for reviewing all alerts and customer transaction patterns and shall conduct Enhanced Due Diligence (EDD) where necessary.
- Assessment of Virtual Assets related business and professional practices: The Company is committed to rigorous assessments on the Customer's transactions with extra focus on the high-risk transactions.
- Assessment of technologies associated with Virtual Assets activities: The Company will conduct a thorough due diligence on the technologies used for Virtual Asset Activities. This includes assessing the security features, protocols, and potential vulnerabilities associated with the underlying technology. The Company also uses Transaction Monitoring System to facilitate risk-based transaction monitoring. The Company will also follow best practices for securing technology infrastructure, including robust access controls, encryption, and other security measures to mitigate against any potential breaches.

e. In respect to the development of new products, business practices and technologies, including new delivery mechanisms, channels and partners; and the use of new or

developing technologies for both new and existing products, the Company must take reasonable steps to ensure that it has:

- assessed and identified the ML risks relating to the product, business practice or technology before its launch; and
- taken appropriate steps to manage and mitigate the risks identified above,

7. AML/CFT Risk Assessment

The Company reviews and understands the ML/FT risks to which they are exposed internally, and how they may be affected by those risks. Specifically, the Federal Decree Law No. (20) of 2018 (AML-CFT Law) provides that they shall continuously assess, document, and update such assessments based on the various risk factors.

A well-documented assessment of the identified risk factors is fundamental to the adoption and effective application of reasonable and proportionate ML/FT risk mitigation measures. The result of such an assessment allows for a systematic categorization and prioritization of inherent and residual ML/FT risks, which in turn allows the Company to determine the types and appropriate levels of AML/CFT resources needed for mitigation purposes.

The AML/CFT Risk Assessment is required to be carried out at three levels namely:

- Enterprise-Wide level.
- Product / Service / Delivery Channel / New Technologies level; and
- Customer Level

7.1 Enterprise-Wide Risk Assessment

The objective of enterprise-wide ML/FT risk assessment is to enhance the efficiency of ML/FT risk management by identifying the ML/FT risks faced by the Company as a whole, determining how these risks are mitigated through internal policies, procedures, and controls, and identifying the residual ML/FT risks that must be addressed.

Effective enterprise-wide risk assessment permits the Company to identify gaps and areas for improvement in its framework of internal AML/CFT policies, procedures, and controls, as well as to make educated management decisions on risk appetite, allocation of AML/CFT resources, and ML/FT risk-mitigation strategies that are aligned with residual risks.

At a minimum on an annual basis, the Company is required to do an enterprise-wide risk assessment and provide the results as well as any risk mitigation plans to the Board.

7.2 Assessing New Product and New Technologies Risks

As part of the Company's obligation to update their ML/FT risk assessments on an ongoing basis, the AML-CFT Decision specifically requires to "identify and assess the risks of ML and FT that may arise when developing new products and new professional practices, including means of providing new services and using new or under development techniques for both new and existing products." Prior to the launch of any new products or services, processes, techniques, or technologies, the Company is committed to maintaining that an assessment of these risks has been conducted and that suitable risk management measures have been taken.

The Company is committed to adopting innovative approaches to effectively implement AML/CFT systems, utilizing advanced technology and analytical tools. Before introducing any new product, service, or technology, the Company will conduct comprehensive risk assessments to identify potential risks. The Company will ensure that all identified risks are effectively managed or mitigated to maintain compliance with the VARA rules and regulations.

7.3 Assessing Customer Risk

The MLRO conducts a risk-based assessment on all Customers, with clear documentation of the process used to determine each Customer's risk rating. This risk rating guides the level of Client Due Diligence (CDD) to be applied.

To assign an appropriate risk rating, the MLRO completes the CDD process prior to establishing any Customer relationship and, where appropriate, for existing Customers on a periodic or event-driven basis. The following sections of this Policy will provide further details on the Company's risk-based approach and the application of CDD measures on Customers.

8. Customer Risk Assessment

Customer risk assessment is done at the following times:

a. Prior to onboarding a new Customer, and

b. Post-onboarding as follows:

- During a scheduled review of an existing Customer;

- Upon Red Flags/suspicious indications during a business relationship with the Customer;
- When information about the Customer, requested services or other circumstances change significantly.

When undertaking a risk-based assessment of a Customer the Company shall:

- Identify the Customer and any Ultimate Beneficial Owner ("UBO");
- Obtain information on the purpose and intended nature of the relationship;
- Obtain information on, and take into consideration, the nature of the Customer's business/background;
- Take into consideration the nature of the Customer, its ownership and control structure, and its Beneficial Ownership (if any);
- Take into consideration the nature of the Customer's existing business relationship (if any) with the Company;
- Take into consideration the Customer's country of origin, residence, nationality, place of incorporation/residence;
- Take into consideration the relevant product, service or transaction;
- Take into consideration the outcomes of AML business risk assessment.

Certain factors may indicate higher ML risks, and other factors may indicate lower ML risk. The Customer's risk level shall be assessed with consideration of all the known factors. The Company's risk assessment consists of a weighted scoring model that quantifies the level of risk each Customer poses on the Company. The Customers' risk score is calculated using a combination of relevant risk factors with assigned weights. Where a Prospective Customer is assessed to be carrying a higher risk, the Company may seek to obtain additional requirements and documentation.

The MLRO may at his sole discretion reject or terminate any business relationship with any of the prospective Customers or Customers, if any of the of the risk factors identified causes any concerns or alerts that the Company deems unsuitable for its business.

8.1 Risk Parameters for Customers

The Company applies a weighted scoring model to assess the risk level of each Customer. The risk score is calculated based on the following factors and respective weights:

Individual Customers Risk Calculation:

Risk Factor	Weight (%)	Description
Nationality	12.5%	Risk rating based on Customer's nationality according to List of jurisdictions in Annexure 2.
Country of Residence	12.5%	Geographic risk linked to Customer's country of residence, referenced against Annexure 2.
Employment Status	12.5%	Risk evaluated based on the Customer's employment or occupational status, considering the source, stability, and transparency of their income.
Product/Services/Activity	6.25%	Risk associated with the specific products, services, or activities the Customer engages in.
Source of Wealth	6.25%	Assessment of the legitimacy, complexity, and transparency of the Customer's source of wealth.
Client Type	6.25%	Risk arising from the Customer's employment type
Country of Origin of Funds	12.5%	Geographic risk linked to Customer's origin of funds, referenced against Annexure 2.
Distribution Channel	6.25%	Consideration of how the Customer was introduced, with particular attention to the digital nature of the company.
Employment Country	12.5%	Risk arising from any the Geographical risk linked to the Customers Country of employment.
Registered Mobile Country Code	6.25%	Risk arising from any the Geographical risk linked to the Customers mobile country code.
Length of Relationship	6.25	Risk arising from any the length of the client relationship.

Corporate Customers Risk Calculation

Risk Factor	Weight (%)	Description
Country of Incorporation	15%	Risk rating based on the country where the Corporate Customer is incorporated, especially if on List A or considered high-risk by FATF or national regulations.
Country of Operations	15%	Geographic risk associated with the jurisdictions where the entity primarily conducts its business.

Operational Status	10%	Risk evaluated based on the Corporate Customer business operational status, considering the source, stability, and transparency of the corporate income.
Nature of Business Activity	10%	Risk associated with the sector, products, or services offered by the Corporate Customer, particularly if involving high-risk industries like virtual assets, gaming, or offshore finance.
Ownership and Control Structure	10%	Risk based on the complexity and transparency of the Corporate Customer ownership, including use of nominees, trusts, or offshore structures.
Source of Funds / Revenue	15%	Evaluation of the legitimacy and transparency of the Corporate Customer funding sources and business revenues.
PEP Involvement	10%	Risk arising from any beneficial owner, director, or senior manager being a PEP or linked to one.
Client Referral Method	5%	How the Corporate Customer was introduced (e.g., directly, by third party, or via a broker), with higher risk from unknown intermediaries.
Tax Compliance Risk	5%	Whether the Corporate Customer is structured or operating in a manner that raises concerns around tax evasion, avoidance, or regulatory arbitrage.
Digital Reputation / Adverse Media	5%	Screening for Adverse Media, legal disputes, enforcement actions, or Sanctions involving the entity, UBOs, or directors.

If a risk rating is adjusted by the MLRO, either higher or lower, based on additional KYC findings, the justification for the change must be documented, along with the MLRO's assessment and conclusion prior to final approval.

8.2 Customer Risk Scoring Methodology

The Company adopts a percentage-based risk scoring methodology to determine the overall risk profile of each Customer, whether an individual or a corporate entity. This approach ensures that the risk assessment is proportionate, consistent, and aligned with applicable UAE AML/CFT regulations and the expectations of VARA.

Step 1: Assigning Risk Rating

Each Customer is evaluated across a set of defined risk factors as mentioned in section 8.1. For

each factor, the Company assigns a risk score on a scale of 1 to 5:

- 1 = Low Risk
- 2–3 = Medium Risk
- 4–5 = High Risk

Step 2 – Applying Risk Weights

Each risk factor is assigned a fixed weight (%) as mentioned in section 8.1. The factor's score is multiplied by its assigned weight to generate a weighted score.

Step 3 – Calculating the Total Risk Score

All weighted scores are summed to determine the Customer's Total Risk Score.

Step 4 – Risk Classification

The Customer's Total Risk Score is then mapped to one of the following risk levels:

Total Risk Score	Risk Level
0.1 to 1.49	Low Risk
1.5 to 2.49	Low to Medium Risk
2.5 to 3.49	Medium Risk
3.5 to 4.49	Medium to High
4.5 to 5	High

Customers rated as High Risk shall be subject to Enhanced Due Diligence (EDD). Customers scoring above 4.5 shall not be onboarded unless otherwise approved by the MLRO and other relevant members of senior management (where relevant) and justified in writing.

8.3 Prohibited Customers

The Company is prohibited from:

- Onboarding any Customer listed on international, regional, or domestic sanctions lists, including those issued by UNSC, EOCN, OFAC, HMT and the EU or under applicable laws and regulations.
- Onboarding any Customer resident in one of the prohibited countries listed in Annex 1.

- Establishing correspondent banking relationships with shell banks.
- Establishing relationships with foreign banks that do not have a physical presence or are not Regulated Affiliates.
- Opening or maintaining anonymous accounts, accounts under false names.
- Opening or maintaining nominee accounts where the beneficial owner is not disclosed.
- Onboarding known or suspected Customers with involvement in criminal activity, including ML/TF or other illicit conduct.
- Onboarding and dealing with Customers associated with Darknet transactions or those presenting heightened reputational risk.
- Onboarding and dealing with Customers located in jurisdictions deemed unacceptable or who fail to comply with identity verification requirements.
- Onboarding Customers with ownership structures that lack transparency, including complex entities, unregulated financial institutions, certain trusts, or individuals seeking to remain anonymous.
- Onboarding Customers who are involved in sensitive or high-risk sectors such as arms trade, illicit drugs (non-medical), or other activities deemed ethically or legally questionable.

9. Implementation of Screening Requirements

The Company shall not deal with any sanctioned person, entity, or funds. And shall follow the below order on Screening:

- The first Sanction check shall be carried out automatically during the Customer's Onboarding Process by the AML/KYC Service Provider against the Sanctions, PEP, and Adverse Media lists provided by the AML/KYC Service Provider.
- Ongoing screening of all Customers is also performed automatically by the AML/KYC Service Provider at least once a day . If a Sanctions, Adverse Media, or new PEP results are identified, the relevant notice will be sent to the MLRO who shall take the appropriate action. The below table clarifies the AML/KYC Provider Screening list updates duration:

Type of data (source)	When the data is reflected in the AML/KYC Provider
Adverse Media	Periodically once the source database is updated.
Sanctions	Within 24 hours after publication on the source website.
Politically exposed persons (PEPs)	Periodically once the source database is updated.

If the MLRO identified that the Customer with a Sanctions nexus, the following actions must be taken:

- Immediately freeze Customer's account on the Company's platform and stop all the transaction(s);
- Immediately file e-STR to the UAE FIU;
- Notify the relevant Regulatory Authority (VARA);
- The Company shall cooperate with the Regulatory Authority (VARA) in verifying the accuracy of information;
- Wait for further instructions from the UAE FIU and VARA;

The MLRO shall also notify the UAE FIU and VARA in the following cases:

- If it was found that one of its previous Customers or any occasional Customer it dealt with, is listed on the Sanctions List or Local Lists.
- If it suspects that one of its current or former Customers, or a person it has a business relationship with is listed or has a direct or indirect relationship with the Listed Person.
- Information relating to funds that have been unfrozen, including their status, nature, value and measures that were taken in respect thereof, and any other information relevant to such decisions.

When identifying the subject of the Sanctions, it is necessary to identify the measures that are taken to Sanction this person. These measures are described in the legal act implementing

the Sanctions; therefore, it is necessary to identify the exact sanction that is implemented against the person to ensure legal and proper application of measures.

10. Customer Onboarding Process

The Company is committed to implementing CDD policies and procedures to safeguard against financial crime risks and exercise due diligence when dealing with Customers. In the course of conducting business, the Company must assist and cooperate with regulators and relevant law enforcement authorities in detecting and preventing ML and TF. The Company's only deals with Customers whose identity is known and verified, Source of Funds is and funds can be reasonably established to be legitimate and whose remittance transactions carry true economic value.

As a result, the Company refrains from opening an account or conducting any transaction for an anonymous or fictitious name or Customer. In addition, the Company refrains from dealing with any anonymous-enhanced transactions.

The Company has developed diligent procedures to verify the identity of all its Customers. Customers are not be allowed to use any of the Company's services offered or deposit any funds prior to completion of the required KYC identification and verification ("Onboarding Process") by the Company. After successful completion of the Onboarding Process, and according to the KYC level of verification attained by the Customer, the Customer will be able to access the services on the Company's portal.

The Company implements a fully compliant and advanced Customer onboarding and AML screening system through dealing with IDWise ("AML/KYC Provider") that is designed to facilitate the process of Customer's identity verification and screening, in order to assess and manage any ML or TF risks associated with the Customer. The Company and the AML/KYC Provider shall simultaneously complete the below Onboarding Process as follows:

- KYC Creation
- Ongoing Sanctions, Adverse Media and PEP screening
- Ongoing document verification and monitoring
- Ongoing identity verification and monitoring
- Liveness check and Face Match

- Email, phone and address verification
- The AML/KYC Provider shall issue automatic KYC application approvals, rejections, return, and delegation to the MLRO. The below is more information on the automatic KYC application action and status:

Automatic KYC Application Status	Description
Approved	Verification is passed successfully and no Red Flags are detected.
Rejected	The Prospective Customer is rejected because of major violations. For example, fraud attempts or Sanctions.
Resubmission requested	The Prospective Customer is required to resubmit certain documents because of minor violations. For example, some of the uploaded documents are of poor quality and the content in the document cannot be recognized. Temporarily rejected Prospective Customers can correct the detected issue and retry passing the Onboarding Process.
Requires action	Manual assistance from the MLRO is required. The Prospective Customer is required to be checked manually because something prevents the Customer from performing the automatic check. For example, some data is incorrect or mismatches were found.

The MLRO reviews KYC applications on a daily basis and has the option to modify the AML/KYC Provider automatic action taken, if necessary.

The Company shall onboard:

- Retail Customers, any legal entity or individual seeking general information and means to access fractional ownership in real estate through regulated ARVAs;

Retail Customers will be referred hereinafter in the Policy as "Customers", unless specified otherwise.

10.1 Customer Onboarding Steps

For use of the Company's services, the Customer shall register at the Company's website and pass the following steps:

1	The Customer shall specify and verify their email.
2	The Customer shall specify and verify their mobile number.
3	The Customer shall upload Identification Document which will be used to verify his full name, date of birth, nationality and place of birth
4	The Customer shall specify and confirm the password, which will be used (together with email or phone number) as login credentials to the Company's website.
5	The Customer shall pass Onboarding Process automatically and remotely.
6	The company shall automatically notify the Customer regarding the result of Onboarding Process. a. If there's no additional actions needed, the Company's AML/KYC Provider shall notify the Customer (through website and e-mail/SMS), that the Onboarding Process has been passed successfully, and the Customer may perform transactions with the Company. b. If any additional actions are needed, the MLRO shall contact the Customer to get more information, if needed. - If the MLRO shall approve the Customer, he shall manually approve the Customer KYC level in the AML/CFT Provider system. After this, an automatic confirmation, that the Onboarding Process has been passed successfully, will be shared with the Customer and the Customer may perform transactions with the Company. - If the MLRO shall reject the Customer, he shall manually reject the Customer KYC level in the AML/CFT Provider system. After this, an automatic rejection will be shared with the Customer. Most of the rejection emails have very limited information so there is no tipping off.

For entity accounts: Onboarding will initially be non-automatic. After review and approval by the Compliance team, the entity account will be created automatically and managed by the system.

10.2 Failure to be approved by the KYC System

There are various reasons as to why a Prospective Customer may be rejected automatically by the AML/KYC Provider. The MLRO reviews the Customer's reasons of rejection and shall either:

- Keep the Customer rejected;
- Approve the Customer as the rejection reasons are not true;
- Require additional information from the Prospective Customer . Then review and assess the information received. After revision and EDD process is complete the MLRO shall approve the Customer manually or keep the Customer as rejected.

11. Customer Due Diligence

The Company undertakes a risk-based ML assessment for all its Customers and assigns a risk rating in proportion to the Customer's ML/TF risks. The ML/TF risk level defines the appropriate level of Customer Due Diligence ("CDD"), simplified or enhanced, to be applied to the Customer. Therefore, the risk assessment procedure is mandatory to ensure sufficiency of the applied level of CDD.

The Customer risk assessment is designed and implemented to assist the Company to better understand their risk exposure posed to the Company .

In case the information received during the Onboarding Process is mismatched or suspicious, the MLRO must postpone the Onboarding Process until the relevant proper assessment is done.

i. Typical CDD processes include the following steps:

- Identifying and verifying all Customers ;
- Performing adequate checks against Sanctions lists;
- Undertaking on-going due diligence of the Customer business relationship;
- Understanding the purpose of the Customer to develop risk profiles;
- Conducting ongoing monitoring to detect and report Suspicious Activity that may arise.
- Verifying that any Entity purporting to act on behalf of the Customer is duly authorized, and verifying the identity of that Entity in accordance with VARA Compliance and Risk Management Rulebook;
- Understanding the intended purpose and nature of the business relationship with the Customer, and obtaining, when necessary, information related to this purpose;

- Where the Customer is a Corporate Customer or provides services to other clientele, understanding the nature of the Customer's business and its ownership and control structure, including but not limited to:
  - The identity of its UBO(s);
  - Whether the structure includes any DAOs and, if so, the intended purpose of such DAOs;
  - The type, nature, and pursuits of the Customer's clientele, and, where necessary, conducting appropriate due diligence on such clientele to ensure compliance with the Federal AML-CFT Laws.

ii. The risk-based approach in accordance with the Federal AML/CFT laws are adopted during CDD.

iii. The Company shall undertake CDD measures in the following circumstances:

- When establishing a business relationship with the Customer for the purposes of providing services relating to Virtual Assets activities;
- When the Customer carries out occasional transactions in amounts equal to or exceeding AED 3,500, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
- Where there is an instruction from Customer to handle a potential Suspicious Transaction;
- Where there are doubts about the veracity or adequacy of previously obtained identification information of the Customer and UBOs; and
- When carrying out any transaction for high-risk Customers as characterised in the Federal AML-CFT Laws.

If the Company is unable to conduct appropriate CDD measures, it shall not establish or maintain a business relationship with the Customer or the Customer shall not execute any transaction on the platform. In the case of receiving information in foreign languages within the framework of CDD measures implementation, the Company may request translation of the documents to another language applicable for the Company. The use of translations may be avoided in situations when the original documents are prepared in a language applicable for the Company.

The level of CDD to be undertaken (both initially and for the duration of the business relationship) is determined by reference to the Customer's risk rating assigned under the Customer Risk Assessment.

11.1 Application of Standard CDD Measures

Standard CDD measures are applied to all Customers. The following standard CDD measures are applied to the Customers:

Initial Standard CDD (onboarding)		
Customer Type	*Information Collected*	*Documents Collected*
Individual Customer	• full name as shown on the Identification Card or Travel Document (including any alias) • Date of birth • Nationality; • Place of birth; • Residencial address; • Occupation; • Name and address of employer; • Customer's selfie; • Face match with the ID provided; • Wealth source *If the Potential Customer is identified as a Politically Exposed Person ("PEP"), approval from the* MLRO *and a member of the Senior Management is required prior to establishing a business relationship with the Customer.*	• Copy of Passport and/or official ID. • Proof of address containing full address information. • Proof of source of funds (if applicable) • Proof of source of Wealth (if applicable).

Initial Standard CDD (onboarding)		
Customer Type	*Information Collected*	*Documents Collected*
Corporate Customer	- Full business name and trade name; - Entity type; - Place of incorporation; - Date of incorporation; - Commercial license number; - Full names of individuals holding Senior Management positions; - UBO name and identification documents. - Source of funds (if applicable) - Source of Wealth (if applicable) *If the UBO is identified as a Politically Exposed Person ("PEP"), approval from the* MLRO *and a member of the Senior Management is required prior to establishing a business relationship with the Customer.*	● Memorandum of association. ● Articles of association. ● Trade license (if applicable). ● Audited reports (if applicable). ● UBO copy of Passport and/or official ID. *All documents shall be attested by competent authorities within UAE.*

Identification of the Customer and verification of the submitted information based on information obtained from a reliable and independent source. This measure is performed in the course of the Customer's Onboarding Process. The Company collects an acceptable identity document, supporting documents and the Customer's Face Match. After the documents are collected, the AML/KYC Provider perform automatic checks related to the authenticity of the documents (whether the document has the appropriate security measures, whether the correct font has been used, if the document is authentic, if graphic editing software has been used for making the document, etc.).

The below table list all data that will be collected from the Customer and the way it will be collected:

Data shall be collected	Collecting requirements	Verification requirements
First and last name(s) / Company full name	Shall be collected automatically through AML/KYC Provider	Shall be verified by AML/KYC Provider's software which performs the Customer's data screening against watchlists and Adverse media.
Personal number/ Company contact number		

Citizenship/ Company incorporation country		
Photograph or Customer's Selfie		
Signature on ID document		
Email	Shall be collected automatically through the Company's application	Shall be verified by sending a verification code by email. The Customer shall enter this code via the platform's function.
Device ID	Shall be collected automatically through the Company's application	Data collected is analysed to establish the following: - operational system used by the Customer; - web browser or other software used by the Customer; - IP address location.
IP address		
Acknowledgment of reading, understanding and agreement with Terms of Service of the Company	The Customer shall confirm this fact by choosing the relevant option on the Company's website.	No additional verification performed.
Consent for personal data processing		
Senior Management and UBOs full names (in case of a Company)	Shall be collected automatically by the Company	Name screening will be done by the AML/KYC provider.

The below table list all documents that will be collected from the Customer and the way it will be collected:

Documents shall be collected	Collecting requirements
Identity Document	The Customer Onboarding Process must be returned or terminated if any of the following circumstances occur:

	● photo of identification document is not taken in real time; ● photo of identification document is interrupted or there are problems with the taking a real time photo; ● the quality of the photo does not allow an accurately see the Customer's picture and/or does not allow the identification of the customer from the facial image on the identity document; ● the identity document is damaged, forged or otherwise suspicious of the authenticity; ● Identity of the Customer does not match the data filled in Customer's KYC.
Customer's Selfie	The Customer Onboarding Process must be returned or terminated if any of the following circumstances occur: ● there are reasonable doubts that the individual in the Selfie and the Customer whose identity is being established are not the same person; ● more than one person is involved in the process of identifying the Customer during the Customer's Selfie; ● the Customer objects to the taking the Selfie; ● The Selfie does not show the Customer's face and/or Customer's face is not clearly visible and distinguishable from objects in the background;
Proof of Address (In case of additional CDD and EDD measures) The following documents are acceptable and include but is not limited to: ● Financial Statements: Bank statement, credit card statement, etc.; ● Letters from Government Bodies: Letters ● from home office, treasury, etc.; ● Bills: Gas, electricity, landline ● telephone, council tax, water, mortgage ● statement, etc.; ● Tenancy agreements: contracts	The following documents are not accepted as proof of address: ● documents more than 6 months old (except tenancy agreements); ● documents that are damaged in a way that the time or content is not easily and clearly identifiable; and ● where there is any suspicion that the document has been distorted by the use of photoshop or any other means.

with andlords renting a property	
Constitutional Documents (in case of an Entity)	The following documents are not accepted: ● Documents that are not stamped by a Regulatory Authority; ● Outdated documents; ● D ocuments that are damaged in a way that the time or content is not easily and clearly identifiable; ● W here there is any suspicion that the document has been distorted by the use of photoshop or any other means.

11.2 Dealing with AML/KYC Provider

The Company acknowledges that the AML/KYC Provider will handle a part of the CDD process. In order to maintain compliance with all applicable laws and regulations, the Company has implemented the following controls to ensure that the AML/KYC Provider performance of CDD is in accordance with all relevant Rules and Directives.

- Overall Liability for the CDD Process: The Company explicitly accepts full responsibility for all CDD procedures. This includes obligations to ensure that the CDD aligns with the relevant requirements, directives, and Federal AML-CFT Laws.
- Ongoing Communication with the AML/KYC Provider: The Company will maintain direct and continuous communication with the AML/KYC Provider. This ensures that the AML/KYC provider is promptly informed of any changes in the nature or size of the business. This proactive communication is vital for the AML/KYC Provider to adjust their processes and methodologies accordingly.
- Role of the MLRO: The MLRO will be responsible for overseeing the KYC applications and the CDD measures in place. This includes a review of the status and alerts raised for both existing and Prospective Customers.

12. Politically Exposed Persons (PEPs)

Politically Exposed Person (“PEP”) means the natural persons who are or have been entrusted with

Prominent Public Functions and close family members or close associates of such persons.

- Prominent Public Functions means:
  - The head of the state, the head of the government, a minister, a vice-minister or a deputy minister, a secretary of the state, a chancellor of the parliament, government, or a ministry;
  - A member of the parliament;
  - A member of the Supreme Court, the Constitutional Court or any other supreme judicial authorities whose decisions are not subject to appeal;
  - A mayor of the municipality, a head of the municipal administration;
  - A member of the management body of the supreme institution of state audit or control, or a chair, deputy chair, or a member of the board of the central bank;
  - Ambassadors of foreign states, a chargé d'affaires ad interim, the head of the UAE armed forces, commander of the armed forces and units, chief of defence staff or senior officer of foreign armed forces;
  - A member of the management or supervisory body of a public undertaking, a public limited company or a private limited company, whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state;
  - A member of the management or supervisory body of a municipal undertaking, a public limited company or a private limited company whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state, and which are considered as large enterprises in terms of the Law on Financial Statements of Entities of the UAE;
  - A director, a deputy director or a member of the management or supervisory body of an international intergovernmental organization; j. A leader, a deputy leader or a member of the management body of a political party.
- Close Family Member means the spouse, the person with whom the partnership has been registered (i.e., the cohabitant), parents, brothers, sisters, children and children's spouses, children's cohabitants.
- Close Associate means:
  - A natural person who, together with the Politically Exposed Person, is a member of

the same legal entity or of a body without legal personality or maintains other business relationship;

- A natural person who is the only Beneficial Owner of the legal entity or a body without legal personality set up or operating de facto with the aim of acquiring property or another personal benefit for the Politically Exposed Person.

If the MLRO encounters a PEP during onboarding, whether it's the Customer, Customer's member of the Senior Management, or Customer's UBO, the MLRO must:

- Undertake EDD;
- Take reasonable measures to establish the source of funds/ source of wealth;
- Increase the degree and nature of monitoring of the business relationship to determine whether the account activity appears suspicious or unusual;
- Obtain the Company's Senior management approval to commence the business relationship;
- Ongoing update of the customer due diligence information.

13. Application of Enhanced CDD Measures

Customers assigned high risk rating in accordance with the Customer Risk Assessment shall undergo Enhanced CDD by the MLRO, in addition to Standard CDD, the following is obtained by the Company:

Initial Enhanced CDD (onboarding) – in addition to Standard CDD requirements		
Requirement	Information	Documents
Obtain & verify additionally the identity of the Customer	• Secondary identification information of the Customer • information on the intended nature of the business relationship	• Secondary ID, e.g. National ID, driving license or similar. • Supporting documents for the proposed service/ transaction as applicable

Initial Enhanced CDD (onboarding) – in addition to Standard CDD requirements		
Requirement	Information	Documents
Establish & verify source of wealth and funds	● the source of funds and wealth, of the individual or Corporate Customer	● Financial statements (if Self-employed), or salary certificate/slips if salary, or inheritance documents/probate if inheritance, etc. as applicable ● Bank statement of the Customer's account showing source of funds and wealth.

Additional CDD measures must be taken in the following events:

- In case the Customer is a PEP: This measure is applied when the Customer, members of Customer Senior Management, or Customer's UBO is identified as a PEP or their family member is a person known to be a close associate. Each Customer, including members of senior management and UBOs, are verified against the PEP watchlists through AML/KYC Provider's software. In addition, this status may be verified manually by the MLRO.
  The PEP status puts the Customer into a high-risk category and makes them subject to enhanced CDD and Enhanced Due Diligence ("EDD"). EDD involves objective, rigorous, and thorough research that provides a greater view of the Customer's profile and the actions required to mitigate higher risks. Such Customers remain high-risk for at least 12 months after they officially cease to be a PEP unless it is established that person still poses a risk specific to PEPs. PEP screening is an ongoing process for all Customers for the length of the Business relationship.
- In case Customer is from a high-risk country or is residing in a high-risk country.

The Company continuously monitors the Customer's risk profile throughout the business relationship to determine whether the application of Enhanced Due Diligence (EDD) measures is applicable.

During the business relationship the Company assesses whether the Customer's risk profile is changed and if the relevant EDD measures shall be applied to the Customer.

When EDD measures must be applied, the amount of EDD measures and the scope of such

measures shall be determined by the MLRO. After application of EDD measures, an approval from the MLRO to establish or continue the business relationship with such Customer(s) must be obtained. In the case of application of EDD measures, the Company monitors the business relationship more often than usual and reassesses the Customer's risk profile every six month, or earlier as decided by the MLRO.

if the Customer has been assigned a "high" risk rating in accordance with the Customer Risk Assessment, the Company must apply the following EDD measures, in accordance with VARA regulations:

- Obtain additional identification information for the Customer and all UBOs;
- Obtain additional information on the intended nature of the business relationship;
- Obtain information on the reasons for the completed transaction(s);
- Update CDD information for the Customer and any UBO more frequently;
- Identify and verify the source of funds of transactions;
- Identify and verify the source of wealth of the Customer and, if applicable, the UBOs;
- Carry out enhanced monitoring of the business relationship by increasing the frequency and intensity of applied controls, and determining which types of transactions require further examination;
- Obtain formal approval from Senior Management before establishing a business relationship or to continue the business relationship, if already established;
- Ensure the first transaction into the Customer's account is conducted through an account in the Customer's name with a licensed financial institution subject to AML/CFT regulations and supervision in a FATF-compliant jurisdiction; and
- For Customers who are natural persons, verify the current residential address.

In addition, and on a case-by-case basis, the EDD measures may include the following:

- Obtaining additional identification documents for the Customer;
- Conducting more regular reviews and updates of information held by the Company;
- Increasing monitoring of the business relationship and transactions to detect unusual or

Suspicious Activity;

- Reviewing pronouncements from governmental bodies and international organizations such as FATF regarding the AML/CFT framework in the Customer's jurisdiction;
- Assessing the Customer's personal and business reputation through publicly available sources or other means;
- Obtaining a letter of reference or certification from a regulated financial institution that has conducted thorough due diligence on the Customer.

14. Application of Ongoing CDD Measures

The Company implements and maintains ongoing CDD measures to all Customers and all their respective transactions in accordance with the Federal AML/CFT laws. To achieve this, the Company shall adhere to the following:

- Continuous Audit of Transactions: The Company will conduct audits on Customer transactions that are carried out throughout the business relationship, ensuring alignment with the Customer information on record. Additionally, the Company will assess the associated risks, with special attention to identifying the source of funds where necessary, as mandated by the Federal AML/CFT laws. The Company will also apply ongoing CDD measures to Customers conducting high risk transactions.

- Regular Review of CDD Records: The Company will continuously review and ensure that the documents, data or information obtained from CDD measures are up-to-date and appropriate by regularly reviewing such records, particularly those of high-risk Customers. This regular review ensures that the records are up-to-date and appropriate for the ongoing business relationship.

- Ongoing sanction screening: The Company will conduct ongoing screening of Customers, Customer's members of Senior Management, and Customer UBO(s), and their transactions against applicable Sanctions lists, including lists issued by the United Nations Security Council, the UAE Cabinet, and other relevant authorities. This screening will occur at the time of onboarding and regularly throughout the course of the business relationship. Any matches or potential hits will be promptly escalated to the MLRO for further investigation and reported to the relevant authorities as required.

14.1 Updating Customer Data

The MLRO/CO shall assess the accuracy and relevance of the Customer information obtained during the course of the business relationship and ensure that it is kept up to date. Information and documentation shall be reviewed and updated whenever deemed necessary. The following measures shall apply:

- Requesting the Customer to confirm that the identification data previously provided remains accurate and up to date;
- Reviewing the Customer's activity when there are behavioural changes (e.g. in the volume or frequency of transactions, use of new payment institutions, or other anomalies) that are inconsistent with the Customer profile or assigned risk rating;
- Performing periodic reviews based on the time elapsed since the Customer's onboarding:
  - For high-risk Customers, a review must be conducted no later than twelve (12) months from the date of onboarding;
  - For medium risk Customers, a review must be conducted no later than two (2) years from the date of onboarding;
  - For low risk Customers, a review must be conducted no later than three (3) years from the date of onboarding;

The Company requires Customers to undergo periodic KYC updates to ensure that all information maintained in its systems remains accurate and compliant. These updates are initiated at defined intervals. Any updates, such as a change in name or residential address, are recorded in the Customer's due diligence profile. Where significant changes occur, including a change in nationality, country of residence, or employment status, the Customer's risk rating is re-evaluated, and relevant screening procedures are repeated. If the reassessment results in a high-risk classification, EDD measures are applied in accordance with the Company's risk-based procedures.

The Company may conduct early or unscheduled reviews if certain risk indicators arise, such as changes in transaction behaviour, updated screening results, Adverse Media, changes in source of funds, or newly identified PEP or Sanctions status. In such cases, the Customer's information and risk profile are re-assessed, and EDD is applied if required.

Where Customer data is deemed outdated or inaccurate, the MLRO must initiate a fresh collection and verification process, in line with the requirements of this Policy and applicable CDD procedures.

14.2 Reclassification of the Risk Status of Existing Customers

A Customer's risk classification may change during the course of the business relationship due to specific events or material changes in the Customer's profile or transactions. The Company is required to promptly update the Customer's KYC information upon the occurrence of risk re-classification or upon receipt of additional KYC documentation or data.

Any updates to the Customer's KYC profile shall trigger a rescreening process conducted by the MLRO and/or the AML/KYC Provider, as appropriate, to reassess the Customer's risk score and determine whether reclassification is required.

The Company retains the right to terminate any business relationship based on the outcome of a risk reassessment.

- Change of Country of Citizenship;
- Change of Country of Residency;
- Change in Occupational Status;
- Change in Customer's Net worth or wealth source;
- Change in Customer's Sanctions or PEP screening results; and
- Change in applicable AML/CFT laws and regulations

14.3 Requirements for Ongoing Monitoring of the Business Relationship

The Company shall assess the Customer's behaviour to identify circumstances which may affect the Customer's risk profile; also to ensure that the transactions executed correspond to the information held by the Company about the Customer, his business, risk nature and source of funds. If such circumstances arise, the MLRO/CO shall reassign the Customer's risk level and apply relevant CDD and EDD measures (if any) or terminate the Business Relationship, if the Customer's risk score is not acceptable by the Company.

The Customer's transactions with the Company shall be monitored in accordance with requirements established for the transaction monitoring section automatically and by the MLRO.

In case of suspicion of ML or TF in the course of interactions with the Customer or their representative, the MLRO shall immediately undergo proper EDD and report the Customer either

internally or externally (as needed).

Ongoing Monitoring is applied in the course of the business relationship established with the Customer. This measure includes the following actions:

- Regular update of information received in the course of CDD measures (including screening against updated watchlists) and re-assessment of the Customer's risk profile;
- Ongoing monitoring of the Customer's transactions and behaviour in the course of the Business Relationship, including real-time monitoring, screening and performed transactions monitoring;
- Identification of the source and origin of the Virtual Assets used in transaction(s).

15. Transaction Monitoring

Given the nature of the business model, which involves the issuance and trading of tokenized real estate assets while accepting and disbursing funds exclusively in fiat currency via regulated banking channels, the Company recognises the importance of robust transaction monitoring measures to detect and mitigate potential financial crime risks.

To this end, the Company has implemented Flagright, a transaction monitoring system ("Transaction Monitoring System") designed to track and assess all transactions processed through the platform. The system enables real-time monitoring of customer activity to identify unusual patterns, potential structuring, or transactions that may be ML, TF, or other financial crimes.

The Transaction Monitoring System provides the MLRO with a user-friendly interface for reviewing alerts, conducting investigations, and documenting actions taken. While Virtual Asset flows are not accepted or processed directly by the Company, the monitoring system is configured to support the Company's compliance obligations by flagging any suspicious fiat transactions that may be indicative of underlying illicit activity.

Each alert generated is categorized based on predefined risk typologies, and the MLRO will assess the severity of the transaction based on its risk category and determine the appropriate next steps, including escalation or filing of STR/SAR.

15.1 Alerts and Risk Indicators

Since the Company exclusively accepts fiat currency through regulated banking channels and only permits fiat withdrawals by Customers, the Company uses fiat-specific transaction risk indicators

to detect and assess Suspicious Activity. The Transaction Monitoring System enables the Company to set and adjust thresholds for these indicators, which are aligned with the Customer's risk profile.

When a transaction exceeds a preset threshold or matches predefined suspicious patterns, an alert is generated. These alerts are assessed based on factors including but limited:

- Transaction amount and frequency;
- Deviation from the Customer's typical behaviour;
- Geographic risk (e.g., transactions executed to/from high-risk jurisdictions);
- Cyclical move of funds (e.g., deposit without investing and subsequent withdrawals)
- Multiple withdrawals within a pre-defined period;
- Known Red Flags (e.g., use of third-party accounts, rapid movement of funds).

15.2 Alert Generation

The Transaction Monitoring System Provider automatically generates an alert when a transaction exceeds a pre-set threshold or matches a defined risk typology (e.g., abnormal amount, frequency, jurisdiction, or customer behavior). Alerts are categorized by severity (e.g., *High Risk*, *Medium Risk*) based on the risk indicator triggered. The following detection scenarios have been implemented:

- Multiple deposits within a short period: Alerts are generated when a Customer makes several deposits over a defined period, indicating potentially unusual activity.
- Large single deposit: Transactions that are significantly above a Customer's normal behaviour may trigger an alert, flagging unusual single deposits.
- Deposits from multiple countries: Alerts occur when the source of funds does not match the Customer's registered country or employment country, especially if funds originate from multiple jurisdictions.
- Frequent withdrawals: Multiple withdrawals within a short timeframe are monitored to detect patterns that deviate from typical Customer behaviour.
- Significant withdrawals: Withdrawals that are unusually large relative to a Customer's normal activity may trigger an alert.
- Withdrawals without corresponding investment: Alerts are generated when withdrawals occur without associated investments, particularly when the behaviour differs from the

Customer's usual activity.

15.3 Notification and Initial Review

The MLRO/CO receives immediate notification through the Transaction Monitoring System Provider dashboard. High-risk alerts are prioritized for urgent review; medium-risk alerts are reviewed in line with internal timelines.

15.4 Alert Analysis and Documentation

The MLRO examines the full transaction history, Customer profile, KYC documentation, documents collected from the Customer, and previous alerts (if any). In addition, the MLRO reviews Adverse Media searches, Sanctions/PEP screening, geographic risk assessment, and review of source of funds documentation if already on file. The MLRO must record all observations, rationale, and decisions made directly in the Transaction Monitoring System Provider using internal comment fields or case notes on each alert, and the reason why the alert was resolved.

15.5 Transaction Monitoring EDD

If the alert is not explainable based on available information, EDD is initiated. This may include:

- Requesting additional documents from the Customer (e.g., SOF/SOW);
- Re-assessing the Customer's overall risk rating;
- Escalating for Senior Management and Board;
- Report the Customer to the UAE FIU and VARA, where warranted, in accordance with the MLRO's assessment of ongoing or significant AML/CFT or any financial crime risk.

All EDD steps and findings must be documented within the alert record.

15.6 Alert Closure

Once sufficient information is gathered and a conclusion is reached, the MLRO updates the alert status as appropriate (see classifications below). Supporting documents must be uploaded or linked in the alert file. Closed alerts must remain accessible for audit and regulatory review and all comments will be kept in records for a minimum period of eight (8) years.

- In Review – the alert is under active analysis.
- Flagged – the alert indicates Suspicious Activity; EDD measures are applied and escalation steps may follow.

- Dismissed – the alert is found to be a false positive or adequately explained by existing Customer information.

15.7 Reporting to Senior Management / Board

All high-risk alerts that result in action (e.g., blocked transactions, EDD, SAR filing) are included in the MLRO periodic report to Senior Management or the Board. The report shall summarize:

- Number and nature of alerts reviewed;
- Actions taken (EDD, SARs, risk rating changes);
- Emerging typologies or trends observed.

15.8 Escalation and Further Action

If the MLRO identifies reasonable grounds for suspicion after review and EDD, the MLRO files a Suspicious Activity Report (SAR) with the UAE FIU and VARA. In serious cases (e.g., suspected fraud or Sanctions evasion), the MLRO may recommend account freezing, termination of the relationship, or referral to law enforcement, subject to internal approval procedures.

15.9 Monitoring Measures

The MLRO shall regularly (on daily basis and weekly basis) assess the Company's transactions with the purpose of identifying complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or visible economic or lawful purpose or that are not characteristic of the given business specifics. In the course of this, the following actions shall be performed:

- If all transactions with the Customer within a specific period (usually – 1 month) exceed the Customer usual turnover limits: the MLRO shall assess, keep the Customer under monitoring, and issue Compliance feedback.
- If indicators of suspicious and/or unusual transactions arise for a Customer already under EDD: MLRO shall assess, conduct further EDD and take action as necessary.
- If the Customer's transactions within a specific period (usually – 1 month) are inconsistent with the Company's knowledge of the Customer, their business and risk profile e.g., abnormal size or frequency for that particular Customer: MLRO to assess, conduct EDD, file an internal report along with taking a decision whether to report an SAR/STR to the relevant the UAE FIU and VARA.
- Any other anomalies in the Customer's behaviour or transactions performed (e. g. many

Customers with specific characteristics within a short period of time, many Customers using the same payment institution, etc.) shall be assessed by the MLRO and the needed action will be taken.

- Prior to entering into any transaction with a counterparty VASP or VASP in the same jurisdiction or any other jurisdiction, the Company shall complete risk based due-diligence on such counterparty in order to mitigate AML/CFT risks, this shall include verifying the counterparty's regulatory status, ownership, governance, and AML/CFT controls.. At any time a heightened risk is identified, this due diligence assessment must be repeated for any transaction

15.10 Criteria for identification of Suspicious Transactions

The below table establishes a list of criteria for identification of ML/TF. Suspicious transactions shall be objectively identified by the MLRO, taking into account Customer activities that they consider may be related to ML and/or TF, Customer and UBO identification, and ongoing Customer monitoring business relationships, including the investigation of transactions that have taken place in such relationships.

In general, the transaction monitoring parameters depend on the: size and frequency of transactions, transaction patterns and trends, the sender or beneficiary, source of funds, and geographical risks.

Below is the criteria list of identification of Red Flags relating to the Customer conduct:

1. At the time of establishment of business relationship, the Customer is reluctant to provide information necessary to establish his identity, conceals the identity of the beneficiary or is reluctant to provide information necessary to establish the identity of the beneficiary, provides documents posing doubts on their veracity, authenticity, etc.
2. Receiving information or documents necessary for monitoring the business relationship from the Customer is difficult: it is difficult to contact the Customer, his place of residence and contact information change frequently, no one can be reached by the phone number provided by the Customer or it is always off, the Customer or his representative do not respond to e-mail messages.
3. The Customer is unable to answer questions about his SOF or certain high-risk transactions.
4. When requested to provide information necessary to monitor his account, the Customer

expresses his wish to close the account.

5. Several Customers are registered at the same address provided by the Customer.

6. Despite engaging in activities related to Virtual Assets, the Customer has little knowledge of virtual currencies, cannot explain the ongoing transactions (signs of a possible victim of fraud).

Below is the criteria list of identification of Red Flags relating to transactions conducted by the Customer:

1. The transactions of the Customer do not correspond to the types of activities specified in the founding documents of the Customer or the usual cooperation with the Company. This criterion shall apply where all of the following circumstances are present:
   a. The Customer carries out activities that are not provided for in the submitted in the Onboarding Process.
   b. When requested by the Company, the Customer fails to provide a reasoned explanation and/or information on the monetary operations of transactions being carried out.
2. The trend of transactions performed by the Customer raises suspicion that it is sought to avoid the reporting threshold. This criterion shall apply where all of the following circumstances are present:
   a. Without a clear reason, the Customer concludes a single or several linked transactions totalling to an equivalent of or more than AED 36 ,7 00 (equivalent to $10,000) or the equivalent of that amount in foreign currency;
   b. When requested by the Company, the Customer fails to provide a reasoned explanation and/or information on the trend of transactions being carried out.
3. The Customer carries out larger-than-usual transaction(s).
4. The Customer requests the amount payable to them be paid to any persons who are obviously unrelated to his usual activities (e.g. to a person who has no family ties or contractual relationship with the Customer).
5. The Customer performs transactions where it is difficult or impossible to identify the beneficiary. This criterion shall apply where at least one of the following circumstances is present:
   a. When requested by the Company, the Customer fails to provide data allowing to identity the beneficiary;
   b. The information provided by the Customer on the beneficiary fails to correspond to the

information available in public or independent registers.

6. The Customer performs transactions without clear economic grounds.
7. The Customer is attempting to deal with beneficiaries that are identified as Prohibited Customer, has Adverse Media screening, or sanctioned.
8. The frequency of small money transfers from different accounts to the account of the Customer increases without clear grounds.
9. The age, job, and financial condition of the Customer who is a natural person fail to correspond to the financial activities carried out by the Customer.
10. The Customer's account is transit: funds deposited into the account are soon transferred out, while other transactions are almost non-existent.
11. International payments are made to a PEP, close associate or family member of PEP without clear economic grounds.
12. Customer conducts transactions to/from parties related to illegal activities such as: Darknet Market, ransomware, fraud, scam, high risk exchanges, high risk jurisdictions.
13. Transactions are carried out with natural and legal persons from countries which have not complied with international treaties and conventions on the non-proliferation of weapons of mass destruction.

Below is the criteria list of identification of Red Flags relating to transactions conducted by the Customer relating to the geographical aspect:

1. Monetary operations or transactions are carried out with natural and legal persons from high-risk countries.
2. The Customer is a permanent resident/registered in a country that is not a member of the FATF or an international organization granted the status of an observer in the FATF and engaged in a fight against ML and TF.
3. The Customer regularly performs transactions with legal persons or organizations registered in the high risk or sanctioned jurisdictions.
4. The Customer's Virtual Asset transactions are initiated from Internet Protocol (IP) addresses from jurisdictions with serious deficiencies in the prevention of ML and TF.

15.11 Ongoing Transaction Monitoring

The Transaction Monitoring System shall support the effective monitoring of fiat transactions carried out by the Company's Customers. Specifically, the system shall:

- Monitor the origin and destination of all incoming and outgoing fiat transactions;
- Provide risk scoring and generate risk indicators based on transaction behavior and patterns;
- Conduct financial data analysis to detect anomalies or Suspicious Activity;

15.12 Evaluation of the Transaction Monitoring System Effectiveness

In adherence to VARA's Compliance and Risk Management Rulebook, the Company shall conduct a thorough evaluation on the Transaction Monitoring System. The evaluation will entail a thorough examination of the strengths and limitations of the tool. Based on the findings, the Company will take the appropriate measures to enhance the control of the transaction monitoring process. The Company might amend the threshold level of each Alert, which can be done internally, to further enhance the effectiveness of the Transaction Monitoring System. In addition, based on the finding the Company shall report back to the Transaction Monitoring System of any issues, concerns, or recommendations that might arise. The Transaction Monitoring Tool does have a customer support team who will be available to handle and reply back to questions and concerns raised by the Company.

The evaluation of the Transaction Monitoring System shall be recorded and properly documented.

15.13 Distributed Ledger Analytics and Transaction Monitoring Controls

The Company shall maintain AML/CFT systems capable of onboarding Customers, monitoring and screening transactions across all virtual asset activities, including the use of distributed ledger analytics tools or other investigative tools where applicable. .The transaction monitoring system, through the use of blockchain and distributed ledger analytics tools, allows the Company to trace wallet activity, assess transaction flows, and identify potential ML/TF risks. The Company utilises Flagright for real-time transaction monitoring and IDWise for customer onboarding and AML/CFT screening, ensuring verification against sanctions, PEP, and adverse media databases. The Company shall periodically review and document the capabilities and limitations of these systems , and design transaction monitoring scenarios and thresholds in line with the FATF Report "Virtual Assets – Red Flag Indicators of Money Laundering and Terrorist Financing" (September 2020 and any subsequent

versions). These measures ensure ongoing monitoring of Customers' interaction with the Company's virtual asset activities and support the timely identification of suspicious patterns.

15.14 Systems Oversight

The Company maintains a comprehensive systems oversight framework designed to ensure operational integrity, accuracy, and continuity across all technical environments. The Company's key controls include:

- Quarterly Reconciliations: System and ledger data are reconciled on a quarterly basis to verify the accuracy of records. This process ensures that records remain accurate, traceable, and aligned with financial and operational integrity standards.
- 24-Hour Automated Consistency Checks: Automated consistency checks are executed every 24 hours to confirm data integrity and system coherence. Any anomalies detected are automatically flagged and escalated for immediate review by the relevant operational and risk management teams.
- Dashboard Monitoring: Dedicated dashboards continuously monitor system performance, data flows, and validation pass rates. These dashboards support real-time oversight, trend analysis, and early identification of irregularities, allowing for proactive issue management.
- Error Alerts and Third-Party Connectivity Monitoring: Automated error alerts are in place to detect and report any disruptions or data transmission failures between the Company and third-party service providers. Such alerts ensure prompt investigation and resolution to maintain system reliability and operational continuity.

The Company will not utilise blockchain systems for onboarding purposes. All client onboarding and verification activities are conducted exclusively through the Company's mobile application, using IDWise as the core AML/KYC solution within the Company's compliance and monitoring framework.

16. Suspicious Activity Reporting

Any Company Employee, acting in the ordinary course of his employment, either knows, suspects or has reasonable grounds for knowing or suspecting that a Customer or a Potential Customer is engaged in or attempting ML or TF, that Employee shall promptly notifies the Company's MLRO and shall provide all relevant details.

- Whenever an employee of the Company has a suspicion of ML, the employee shall prepare and file the internal Suspicious Activity/transaction report (i-STR) to the MLRO (Refer to

Appendix 1 for the format of the i-STR). The Employee shall provide as much detail and supporting documents (if any) as possible.

- The Employee shall refrain from conducting any personal investigation and must leave these matters to the MLRO. An uncoordinated or unauthorized investigation may raise suspicion or inadvertently alert the Customer, which could constitute an unlawful tip-off.
- The requirement to report an i-STR to the MLRO applies even if no business relationship has been entered into.
- The suspicions may arise in respect to a single transaction or a continuous activity. While the i-STR form is used for reporting of both, the MLRO in the next step of filing information to the UAE FIU and VARA will distinguish and report either a STR or SAR.
- Employees must not discuss or disclose any suspected activity or the report submitted to the MLRO with anyone employed by the Company or not employed.
- Employees shall be aware that they are strictly prohibited from tipping off any Customer or third party about a suspicion, an internal report, or any AML/CFT investigation or reporting activity.
- The responsibility remains with the Employee to decide whether an i-STR to the MLRO should be made.
- A disciplinary action shall be taken against an Employee who fails to submit an i-STR to the MLRO despite having suspicion of ML.

The MLRO holds the responsibility to report any transaction or activity that, after proper assessment, is known, suspected, or reasonably suspected to be linked to ML, TF, proliferation financing, or any other criminal conduct. In this case, the MLRO, without delay shall:

- Documents the circumstances in relation to which the i-STR has been made;
- Determines whether in accordance with Federal AML legislation an e-STR must be made to the UAE FIU and VARA and documents such determination in the i-STR;
- If required, makes an e-STR/ SAR to the UAE FIU and VARA via GoAML platform or by any other means approved by the UAE FIU and/or VARA as soon as practicable; and
- If the MLRO decides to make an e-STR/ SAR, he should notify the and obtain the Senior Management approval. Failure to report suspicions of ML may constitute a criminal offence that is punishable under the laws of the UAE.

Where the MLRO has reasonable grounds to suspect that a transaction, or an attempted transaction, involves the proceeds of crime or is intended to commit, conceal, or benefit from a crime, the MLRO shall immediately file a SAR/STR with the UAE FIU through the goAML portal.
After submitting the report, the MLRO shall:

- Respond to any information or action requests from the FIU or VARA within forty-eight (48) hours, or within any shorter timeframe specified by those authorities;
- Undertake any additional steps required by the FIU or VARA; and
- Where the MLRO and Compliance Officer are separate individuals, promptly inform the Compliance Officer that an STR has been filed, provided that such notification does not constitute tipping-off under applicable laws.

In the preparation of an e-STR/SAR, if the Company knows or assumes that the funds which form the subject of the e-STR/ SAR do not belong to the Customer but to a third party, this fact and the details of the Company's proposed course of action in relation to the case should be included in the e-STR/ SAR.
If the MLRO has reported an e-STR/ SAR to the FIU and VARA, it must, in accordance with the Federal AML legislation, provide any additional information requested by the UAE FIU. The UAE FIU may instruct the Company on how to continue its business relationship with the reported Customer, including effecting any transaction with a person. If the Customer in question expresses his wish to move the funds before the Company receives instruction from the UAE FIU on how to proceed, the Company should immediately contact the FIU for further instructions.
The MLRO responsibilities extend from filing the e-STR/SAR to documenting the procedures governing the monitoring and reporting of suspicious transactions. This documentation will be then subjected to regular reviews and updates to maintain its efficiency over time. Before implementing new measures or making significant changes to the reporting procedure, the MLRO shall seek the necessary approval from Senior Management, ensuring that the Company's Senior Management is informed and supportive of the proposed changes. The changes might be related to enhancement of communication channels, automation and technology upgrades, or any other adjustments that the MLRO deems imperative for optimizing the reporting process.
The approval from Senior Management is in place to strengthen the Company's capacity to identify and report potentially illicit financial activities in strict adherence to the VARA Compliance and Risk Management Rulebook, thus upholding regulatory compliance and best practices in the field.

Where the MLRO concludes there are no reasonable grounds to suspect money laundering, then consent will be given for ongoing or imminent transaction(s) to proceed.

The MLRO shall maintain all i-SARs, i-STRs, and all related submissions to the FIU and VARA in a secure and confidential file. These records must be retained for a minimum period of eight (8) years. In cases where an investigation related to any SAR or STR remains ongoing beyond the eight-year period, or where the FIU or VARA issues a specific instruction to retain documents related to a particular Customer, the MLRO shall ensure continued secure retention of the relevant records beyond the standard retention period.

16.1 GoAML

In March 2019, the FIU of the UAE conducted an introductory session on GoAML, its new reporting system, to the entities subject to AML regulations in the DIFC. GoAML is a United Nations Office of Drug and Crime (UNODC) developed software that is used by financial intelligence units worldwide. All AML-reporting entities in the UAE (including the Firm) are required to submit various types of informational reports, including Suspicious Transaction Reports and Suspicious Activity Reports, electronically to the UAE FIU and VARA using the GoAML portal. The introduction of such a system enables the FIU to:

- Strengthen and broaden its capability to meet and discharge its legislative objectives and functions;
- Ensure that the UAE's financial system stays relevant and effective in the fight against ML;
- Collaborate more effectively with various stakeholders such as reporting entities, supervisory bodies and law enforcement agencies; and
- Standardise and streamline all reporting requirements and ensure that the UAE is aligned with the AML/CFT standards of FATF.

Additionally, the introduction of the aforementioned system brings in various benefits to its end-Customers, including, but not limited to, the following:

- It facilitates the management of the reporting entities' registration information;
- It introduces a single and standardised reporting definition and format for all reporting types;
- It simplifies failed reporting by requiring the user to only re-submit the remediated failed report; and

- It gives the Customer the ability to communicate with the FIU in a centralized manner through the 'Message Board' function.

16.2 Tipping Off

The Employees are well trained that in accordance with the Federal AML legislation, the Company or any of its Employees must not disclose, directly or indirectly, to the Customer or to any other person that they have reported, or are intending to report, a STR or SAR. They also must not disclose information contained in the e-STR or the fact that a suspicious transaction/activity is being investigated.

If the MLRO reasonably believes that performing CDD measures will tip-off Customer or Potential Customer, the MLRO may choose not to pursue that process and should file an e-STR. The Company ensures that its Employees are aware of and sensitive to these issues when considering the CDD measures.

17. Travel Rule

The Company recognizes that the Travel Rule, as stipulated under VARA's Compliance and Risk Management Rulebook and FATF Recommendation, applies to all transfers of VAs with an equivalent value exceeding AED 3,500, regardless of whether the original funding is in fiat or crypto. As the Company's operations involve the issuance and transfer of real estate tokens, it is committed to ensuring full compliance with Travel Rule requirements.

The Company will collect the below information, which will be made available without delay to VARA and/or other competent authorities upon request.

Originator information shall include, at minimum:

- Full name;
- Account number or Virtual Asset wallet address; and
- Residential or business address.

Beneficiary information shall include, at minimum:

- Full name; and
- Account number or Virtual Asset wallet address.

The Company will evaluate and address risks related to customer deposits and withdrawals, interactions with unhosted virtual asset wallets, and transactions involving enhanced anonymity features. These controls form part of the Company's broader AML/CFT monitoring framework and support adherence to international and VARA standards.

For transactions involving un-hosted, non-custodial, or self-hosted wallets, the Company will:

- Apply a risk-based approach and implement additional mitigation measures where necessary;
- Obtain originator/beneficiary details directly from the Company's customer, as follows:
  - When initiating a transfer to a self-hosted wallet, require the originator customer to identify the intended beneficiary;
  - When receiving a transfer from a self-hosted wallet, require the beneficiary customer to identify the originator.
  - Utilize the Company's transaction monitoring and blockchain analytics tools to assess and document the risk profile of such transactions.

Factor identified	Measures shall be taken
The Customer's wishes to make transactions equal to or exceeding AED 35,000 (equivalent to $10,000) or the equivalent in another currency within 24 hours	MLRO shall ask about SOF and further documentation as applicable.
The Customer wishes to make a transaction equal to or exceeding AED 3,500 (Equivalent to $1,000)	As per VARA Travel Rule, the Company will require the below: ● Originator's: - name; - account number; and - residential or business address. ● Beneficiary's: - name; and - Wallet address.

18. Training and Staff Management

The MLRO is obliged to and ensures to provide Compliance and AML/CFT training to all relevant Employees, Senior Management, and Board at appropriate and regular intervals:

- Within 30 days of joining the Company
- Annually;
- Upon significant changes in applicable AML/CFT legislation;
- Upon significant changes in the Company structure;
- Upon updating the operational policies and procedures of the Company.

The provided training must enable the Company's Employees, Senior Management, and Board to:

- Understand this Policy and other Compliance Policies related to the Company;
- Understand relevant legislation relating to ML and TF;
- Understand Company's policies, procedures, systems and controls related to AML/CFT and any changes to these;
- Recognise transactions and other activities which may be related to ML and TF;
- Understand the types of activity that may constitute Suspicious Activity;
- Understand what is Tipping off and how to avoid it;
- Understand their obligation regarding the making of an i-STR, i-SAR, and other notifications to the MLRO;
- Be aware of the prevailing techniques, methods and trends in ML and TF relevant to the business of the Company;
- Understand the roles and responsibilities of all Employees in combating ML and TF, including the identity and responsibility of the Company's MLRO, and deputy MLRO; and
- Understand the relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions described in Sanctions, International Obligations; and
- Be aware of the consequences of non-compliance with the AML/CFT regulations on Employees, Senior Management, Board, and Company as a whole.

MLRO shall ensure that the AML/CFT training:

- Is appropriately tailored to the Company's activities, including its products, services, Customers, distribution channels, jurisdictions, business partners, level and complexity of its transactions; and
- Indicates the different levels of ML and TF risk and vulnerabilities associated with the above-listed matters;
- Suitable for the duties which the Employees are required to perform in their role.
- Properly record keep and keep track of all trainings held, along with Employees list who attended the training.

19. Staff Management

The Company shall, as per VARA Compliance and Risk Management Rulebook:

- Employ appropriate numbers of Employees to discharge relevant duties effectively;
- Implement procedures to ensure that they only employ suitably qualified individuals with the requisite skills, knowledge and expertise to perform the duties for which they are employed for.
- Ensure that the Company does not prejudice an Employee who discloses any information regarding ML and TF to the VARA or to any other Relevant Authority (such as FIU, a Dubai or Federal Ministry) involved in the prevention of ML.

20. Communications with the VARA

The Company and its Employees shall communicate with the VARA in an open and cooperative manner and in English. The standard communications channel is the VARA Portal.

21. Handling Third Party and Outsourcing

The Company is aware of the risks associated with outsourcing various services and products, due to the presence of highly sensitive data that can be accessed by Employees and the third-party vendors.

In order to keep proper oversight and track of any outsourced third-party operations, the Company has partnered only with third party service providers in which the operation of any Employee or

individual accessing the third-party provider system is recorded immediately after successful logging in to the system. All actions and activities carried out by Employees or individuals who are accessing the third-party providers' platforms will be monitored and logged. In addition, the third-party vendors have disclosed the nature and extent of their security features that safeguard the Customers' information and data. The third-party vendors also have a complete Policy documentation which details their proper security protection through which all Company's data will be protected.

In addition to the above, the Company has drafted a comprehensive Outsourcing Agreement which will be signed with any third party the Company will deal with, the Outsourcing Agreement shall protect the Company Data, Company Materials, Company Software, and Company System. In addition, the Outsourcing Agreement has a comprehensive Data Protection and Confidentiality sections that safeguard the Company.

22. Record Keeping

The Company keeps original and true copy of all documents and information collected. The documents and information include the following:

- Documents and data relating to all transactions whether local or international, including the amount, date, Virtual Asset currency, Wallets addresses of originator and beneficiary, names, fees and charges, and Customer information.
- Documents and matters under investigation or which has been subject to STR/SAR as it may be necessary to the FIU or any other Regulatory Authority.
- All Customer information produced by third parties.
- All records that prove that the Company is operating in compliance with all applicable laws and regulations.
- General Ledger information containing all assets and Virtual Assets, liabilities, ownership equity, income and expense accounts.
- Board minutes of meeting;
- All Customer communication especially regarding handling Customers' complaints and resolution.
- All Conflict of Interest in special register as per the Company rulebook.
- All records of all transactions, policies, procedures, documents, and Customer information.

All documents and information shall be stored in a readily retrievable format for eight (8) years, or for an indefinite period of time if the records relate to the national security of the UAE. All records will be stored in efficient accessible manner and will be made available to VARA and relevant authorities upon request.

Appendix 1- i-STR

This establishes the form of a report that the Employee must fill in and forward to the MLRO in cases specified in AML Policy. The MLRO must accept the report and the documents attached to it and consider the need to send a notification to the competent authority or, if necessary, perform other activities.

EMPLOYEE DETAILS
Name of the Employee sending report:

CUSTOMER'S DETAILS
The Customer's name:
Personal identification code or date of birth/registration code:

TRANSACTION DETAILS
Transaction amount:
Transaction time:
Transaction description:

ADDITIONAL INFORMATION AND GROUNDS FOR DOUBT:

THE AML OFFICER RESOLUTION AND PERFORMED ACTIVITIES
Notification arrival date:
Performed actions:

Appendix 2

High risk and prohibited countries. Country risk scores are derived from Know Your Country, which takes into various considerations such as ML, TF, ABC and other risks. All FATF Grey Listed countries are considered as high risk. Prohibited countries are countries that have been as assessed as “Black” by FATF and countries that have been economically sanctioned by major sanctions issuing authorities.

All risk rated countries - https://www.knowyourcountry.com/country-reports/
High risk rated countries - https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html
Prohibited risk rated countries - https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html and Iran, Cuba, Democratic People's Republic of Korea and Syria.