SUNMONEY
Solar Group

SUNMONEY SOLAR GROUP

SunMoney Solar FZ LLE, SunMoney Solar GMBH, SunMoney Solar PTE LTD, SDBN DMCC, Digitalismunkatars LTD and all their subsidiaries

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM POLICY

Compliance/AML/KYC Partner:

VAF COMPLIANCE

CONTENTS

1	INTRODUCTION

1.1 Introduction

(1) Cryptocurrencies have emerged as a revolutionary form of digital assets that operate on decentralized networks, using cryptographic principles to secure transactions and control the creation of new units. While cryptocurrencies offer numerous advantages, such as faster and cheaper cross-border transactions and increased financial inclusion, they also pose challenges in terms of money laundering and illicit activities. Money laundering involves the concealment of the true origin and ownership of criminal proceeds, allowing perpetrators to evade prosecution, maintain control over illicit funds, and continue their unlawful activities. It is crucial to address these concerns and ensure the responsible and legitimate use of cryptocurrencies.

(2) Involvement in money laundering, whether intentional or unintentional, carries significant consequences, including but not limited to severe reputational damage to individuals, organizations, and the broader cryptocurrency ecosystem. Therefore, it is imperative for all participants, including **SUNMONEY SOLAR GROUP**, to prioritize compliance with relevant laws and regulations aimed at preventing money laundering. By doing so, **SUNMONEY SOLAR GROUP** can safeguard its reputation, protect its stakeholders, and contribute to the overall integrity and trustworthiness of the cryptocurrency industry.

(3) **SUNMONEY SOLAR GROUP** recognizes the utmost importance of adhering to applicable laws and regulations for the prevention of money laundering. **SUNMONEY SOLAR GROUP** is committed to implementing robust policies and procedures, as outlined in this Manual, to prevent its cryptocurrency business from being exploited for criminal activities. By actively promoting compliance and employing stringent measures, **SUNMONEY SOLAR GROUP** aims to create a safe and transparent environment for cryptocurrency transactions, fostering trust among its users and contributing to the wider adoption and acceptance of cryptocurrencies as a legitimate form of digital value transfer.

1.2 About this manual

(1) The Anti-Money Laundering Procedures Manual ("Manual") provided herein is specifically designed for employees involved in the crypto currency business. This Manual applies to all employees within the organization, encompassing members of the Board of Directors, senior managers, operational staff, employees who have customer contact or handle customer transactions, and any other employees who may come across money laundering activities in the course of their work

(2) The purpose of this Manual is to establish comprehensive guidelines and procedures to assist employees in preventing money laundering and adhering to relevant anti-money laundering laws and regulations within the context of crypto currencies. It serves as a vital resource for employees to understand their responsibilities and obligations when dealing with potential money laundering risks within the crypto currency business.

(3) By following the protocols and instructions outlined in this Manual, employees contribute to the organization's commitment to effectively combat money laundering. It is imperative that all employees familiarize themselves with the content of this Manual and diligently implement the prescribed measures in their respective roles. This collective effort reinforces the

organization's dedication to maintaining a robust anti-money laundering framework specific to the crypto currency sector and ensuring compliance with legal requirements.

(4) This Manual has been specifically developed to ensure that employees have a clear understanding of their obligations and SUNMONEY SOLAR GROUP requirements for complying with laws and regulations pertaining to the prevention of money laundering and terrorism financing in relation to crypto currencies in the UAE. It outlines the actions that employees must take to remain compliant and provides guidance on how to identify and report any suspicious activities that may indicate potential money laundering or terrorism financing.

(5) In cases where employees require further assistance or have questions related to anti-money laundering procedures, they should seek guidance from the designated Money Laundering Reporting Officer (MLRO). The MLRO serves as the main point of contact for any concerns or inquiries regarding money laundering issues within the organization. The contact details of the MLRO are as follows:

Role	Name	Email	Mobile
Compliance			

(6) Employees are encouraged to consult with the MLRO whenever necessary to ensure compliance with anti-money laundering regulations and to promptly report any suspicions or observations related to potential money laundering or terrorism financing activities. The MLRO plays a crucial role in providing guidance and ensuring that SUNMONEY SOLAR GROUP maintains a strong anti-money laundering framework within the context of crypto currencies.

1.3 Applicable laws and regulations

(1) The Company will establish and implement policies and procedures to comply with all AML/CFT requirements and existing applicable laws, regulatory requirements and guidelines, including but not limited to

a) the UAE Federal AML-CFT Laws;
b) 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];
c) FATF's Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers [July 2021];
d) FATF's Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [October 2021];
e) the International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, The FATF Recommendations [March 2022];
f) 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;
g) the UAE Executive Office for Control & Non-Proliferation [EOCN] Guidance on Counter Proliferation Financing for FI's, DNFPBs, and VASPs [March 2022]; and
h) the EOCN's Local Terrorist List, as may be amended from time to time.

1.4 Offences and Penalties

(1) The specific offences and penalties for non-compliance with crypto currency regulations in the United Arab Emirates (UAE) can vary depending on the applicable laws and regulations. It is important to consult the relevant legislation and seek legal advice for more precise details. Some general information on potential offences and penalties related to non-compliance with crypto currency regulations in the UAE are

(1.1) Operating without Proper Licensing: Engaging in crypto currency-related activities without obtaining the necessary licenses or permits required by regulatory authorities can lead to legal consequences. This may include conducting crypto currency exchanges, offering crypto currency-related services, or operating crypto currency platforms without proper authorization.

Penalties for operating without the required licenses can include fines, regulatory sanctions, suspension or revocation of licenses, and potential imprisonment depending on the severity of the violation.

(1.2) Failure to Comply with AML/CFT Requirements: Non-compliance with anti-money laundering (AML) and counter-terrorism financing (CFT) obligations, including failure to implement proper Know Your Customer (KYC) procedures, record keeping, and reporting suspicious transactions, can result in significant penalties.

Penalties for AML/CFT violations can include fines, regulatory sanctions, suspension or revocation of licenses, and potential imprisonment depending on the severity and impact of the non-compliance.

(1.3) Fraudulent Activities: Engaging in fraudulent activities or scams involving crypto currencies, such as Ponzi schemes, pyramid schemes, or misleading investors, can result in legal consequences.

Penalties for fraudulent activities can include fines, legal action, asset seizures, and potential imprisonment depending on the severity and impact of the fraud.

(1.4) Violations of Consumer Protection Laws: Failure to adhere to consumer protection laws, such as providing misleading information, misrepresentation of investment opportunities, or unfair business practices in the context of crypto currency offerings, can lead to legal consequences.

Penalties for consumer protection violations can include fines, legal action, compensation orders, and potential imprisonment depending on the severity and impact of the violation.

(2) **SUNMONEY SOLAR GROUP** is aware that the UAE government and regulatory authorities have been

Actively enhancing their regulatory framework for crypto currencies, and the specific offences And penalties may evolve over time. To ensure accurate and up-to-date information, it is crucial to refer to the relevant legislation and consult with legal professionals or regulatory authorities specializing in crypto currency regulations in the UAE.

2	SCOPE

2.1 Scope

This Policy applies to all activities and operations of the Company, to its employees and every other person, including temporary, working for the Company, as well members of the Board, shareholders, consultants, vendors, contractors, and/or any other parties with a business relationship with the Company. The Company shall take steps to ensure that all other entities that participate in the implementation of the Company's activities have policies that are consistent with this Policy.

2.2 Terminology

AML/CFT	Anti-Money Laundering and Countering the Financing of Terrorism
Business Relationship	any existence of a contract providing for the performance of several successive operations or creating continuous obligations, or, in the absence of a contract, by the regularity of the client's intervention.
Client	natural or legal persons (Business Relationships and occasional customers) that have completed the on-boarding procedure for investing in crypto assets or that apply for investing in crypto assets with the Company
CRA	Client Risk Assessment
Crypto asset(s)	A digital representation of value that may be digitally traded, transferred, or used by means of a distributed ledger technologies as an exchange or payment tool, or for investment purposes.
Client Due Diligence	The process to identify and verify the true identity of the Client. This would enable the Company to assess and evaluate the extent of AML/CFT risk associated with the Client, along with the monitoring of transactions during the client relationship, to assess whether the transactions are in line with the customers profile
CASP	Crypto Asset Service Provider
Financial Intelligence Unit (FIU)	Serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis.
Financing of Terrorism (TF)	Is a collective term that refers to various acts with the ultimate purpose of which is to provide material resources to make terrorist activities possible
Know Your Customer (KYC)	Means the identification process to identify the Clients (if applicable, the beneficial owner) integrated within the AML/CFT controls

Money Laundering (ML)	a) the conversion or transfer of property, knowing that such property is derived from crime, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of the crime to evade the legal consequences of his or her actions b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing such property is derived from crime c) the acquisition, possession or use of property, knowing at the time of receipt that such property was derived from a criminal offence.
Compliance Officer (CO)	The person in charge of implementing and supervising the AML/CFT policy within the Company. The CO must be a person occupying a high hierarchical position and possessing sufficient knowledge of the risk exposure affecting the Company's services. He or she also implements the control over AML/CFT service providers.
PEP	'Politically Exposed Person' is a natural person who holds, or has held, a high public office position within the last 12 months. This includes the following: a) heads of state, heads of government, ministers and deputy or assistant ministers b) members of parliament or of similar legislative bodies c) members of the governing bodies of political parties d) members of supreme court, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances e) members of courts of auditors or of the boards of central banks f) ambassadors, chargés d'affaires of high-ranking officers in armed forces g) members of the administrative, management or supervisory bodies of State-owned enterprises h) directors, deputy directors and members of the board or equivalent function of an international organisation. 'Family members' that are treated as PEP include the following: a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person b) the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person c) the parents of a politically exposed person 'Persons know to be close associates' that are treated as PEP: natural persons who are known to have joint beneficial ownership of legal

	entities or legal arrangements, or any other close business relations, with a politically exposed person natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for de facto benefit of a politically exposed person.
POA	Proof Of Address
PSOF	Proof Source Of Funds
POW	Proof Of Wallet
Risk Based Approach (RBA)	the process of identifying, assessing and understanding ML/TF risks to which the Company is exposed and to take measures appropriate to those risks to mitigate them effectively
Tipping-off	disclosing the fact to the counterparty that a suspicious transaction or related information is filed with management or the authorities.
US Person	"United States Person" is generally defined as a natural person who is permanently resident in the United States. and / or any (legal) entity or organization organized in the U.S. or is incorporated under the laws of that country. U.S. Citizens Residing Outside the U.S. may also qualify as a "US Person" under certain regulations.

3 CLIENT DUE DILIGENCE

3.1 CDD

CASP are required to identify and verify the identity of all Clients.

For the Client Due Diligence process the Company verifies the identity documentation and screening for PEP-hits, Sanctions lists). The Company identifies and verifies the identity of their applicants through CDD and carries out ongoing monitoring on their clients to identify anything which might give rise to a suspicion of money laundering or terrorist financing when:

- establishing a business relation
- there is a suspicion of money laundering or terrorist financing
- doubts about the veracity or adequacy of previously obtained Client identification
- when carrying out occasional transactions in favour of a client for 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
- when carrying out any transaction for high-risk clients as characterised in the Federal AML/CFT Laws.

The Company performs CDD, as determined on a risk-based approach, considering the type of Client, Client relationship, financial instrument and country of residence/operation in order to identify their applicants/Clients and ascertain information pertinent to doing business with them.

Due to the non-face-to-face nature of the way in which applicants are onboarded, the Company treats all applicants/Clients at least as “medium risk”. For “high risk” Enhanced Due Diligence (EDD) is a requirement. The Company distinguishes between the different types of applicants/clients and the different types of risk they pose, within the high-risk category there are different levels of risk, designating medium, high and severe risk.

The Company conducts ongoing due diligence on the business relationship and transaction monitoring throughout the course of the relationship to ensure that the transactions being conducted are consistent with the Company’s knowledge of the client and its business and risk profile, including, where necessary, the source of funds.

3.1.1 Identification and verification of a natural person

Client identification and verification requires checking reliable, independent source documentation, data or information that confirms the veracity of the identifying information that was obtained during the identification process, such as documents from a governmental institution or a respectable court. The Company requests the following documentation:

- valid passport, identity card, driving license, OR
- travel documents for refugees and foreigners’ documents

Additional documentation can be requested to verify information other than the identity, for instance, proof of address or source of funds:

- Salary slip
- Bank account statement
- Utilities bill

For the personal details of the applicant, the following information is obtained:

- Full name
- Date and place of birth
- Country of nationality
- A copy of the document that contains a person identification number and which has been used to verify the identity of the applicant
- Full Address
- if the client is a Politically Exposed Person, approval from the CO and a member of the Senior Management is required prior to establishing a business relationship with such client;
- the intended purpose and nature of the business relationship.

For the verification of the main source of funds, the following options can be chosen:

- Income
- Savings
- Gift
- Inheritance
- Other

For the address information, the Client shall provide:

- Address Line 1 (street address and number)

- Address Line 2 (apartment or building)
- City
- Region
- Postal Code
- Country

In case of 'suspicion' Customer Support can request the applicant/client to send an additional selfie via email holding a piece of paper with the date and their ID.

3.1.2 Identification and verification of a legal entity

The Company shall collect the following information about the Client who is a legal entity:

- the name and type of the legal person;
- principal place of business;
- the registry code or registration number and the date of registration;
- the names of the senior management board members or other body replacing the management board, and their authorisation in representing the legal person;
- the ultimate beneficial owners (UBO) of the legal person (if the UBO is a Politically Exposed Person, approval from the CO and a member of the Senior Management is required prior to establishing a business relationship with such client.)
- understand the intended purpose and nature of the business relationship.

The Company verifies a legal person based on the following documents:

- constitutional documents [e.g., memorandum of association and articles of association] attested by competent authorities;
- registry card of the legal person or similar document issued by a public authority.

Where the Company has access to the commercial register or the data of the relevant registers of a foreign country, the submission of the documents specified in this subsection does not need to be demanded from the Client.

A representative of the Client, at the request of the Company, submit a document certifying his or her powers, which has been authenticated by a notary or in accordance with an equivalent procedure and legalised or certified by a certificate replacing legalisation (apostille), unless otherwise provided for in an international agreement.

To verify the identity of the Client's senior management board members, a representative of the client or UBOs, the Company:

- performs same measures as when the Client is a natural person;
- (for UBOs only) request for an extract from the register of beneficial owners, if it is available in the country of incorporation of the legal entity.

Where the Company's client is a business or otherwise provides services to other clientele, understand the nature of the client's business as well as the client's ownership and control structure, including but not limited to the following:

a.) the identity of UBO[s];

b.) whether such structure includes any decentralised autonomous organisations (DAOs) and, if so, the intended purpose of such DAOs;

c.) the type, nature and pursuits of the clientele of a prospective client and where necessary carry out appropriate due diligence on the client's clientele in order to ensure compliance with the Federal AML-CFT Laws.

3.1.3 Verification of Crypto wallet Identity

When verifying the identity associated with a crypto wallet, it is important to gather the following information:

1.) Full Name: The legal name of the individual or entity associated with the crypto wallet.

2.) Date of Birth (DOB): The date of birth of the wallet owner for verification purposes.

3.) Address: The residential or business address linked to the wallet owner.

4.) Government-issued ID: A scanned or photographed copy of a valid government-issued Identification document, such as a passport or driver's license. This helps confirm the identity and age of the wallet owner.

5.) Selfie or Photo: A recent photograph or selfie of the wallet owner holding their government-issued ID next to their face. This provides an additional layer of verification and helps prevent identity theft.

6.) Proof of Address: A document that verifies the address provided, such as a utility bill, bank statement, or official government document issued within the last three months.

7.) Source of Funds: Information regarding the source of funds used to fund the crypto wallet, such as bank statements or documentation indicating the origin of the funds.

8.) Transaction History: A record of previous transactions made from the crypto wallet, including incoming and outgoing transfers, to establish a history of wallet usage.

It is essential to handle and store this information securely, adhering to applicable data protection and privacy regulations. Additionally, it is important to inform the wallet owner about the purpose of collecting this information and how it will be used for verification purposes only.

Additionally, the Company uses a tool that can detect whether an external wallet is owned by a known identity, entity or third-party provider that is linked to high-risk activity. With these tools the KYC Team can perform an enhanced due diligence on the external wallets that are linked to the external wallet of the client to investigate if this client has received funds that are linked to severe and high-risk activities in the past. All incoming and outgoing crypto transactions will be monitored.

3.1.4 Source of funds

SUNMONEY SOLAR GROUP are aware with all important information regarding the verification process for the source of funds associated with crypto wallet identity, particularly for high-risk clients, In accordance with UAE law and regulations.

As part of SUNMONEY SOLAR GROUP commitment to maintaining a robust compliance framework, it is a legal requirement for high-risk clients to provide additional documentation from a reliable and independent source to verify the legitimacy of the source of funds. The statements and evidence provided by the client will be carefully reviewed and added to their client file, ensuring adherence to the relevant laws and regulations.
In determining the plausibility of the source of wealth or funds, several specific indicators will be taken into consideration, including the client's *age, occupation, business activities, and country of origin*. These factors assist in establishing a comprehensive understanding of the client's financial profile and contribute to SUNMONEY SOLAR GROUP commitment to regulatory compliance.

To gain sufficient insight into the source of funds of the clients, SUNMONEY SOLAR GROUP should collect all relevant information necessary for assessment. Examples of documentation that may be collected, but are not limited to, include:

1.) Activity Information: Details pertaining to the client's business or professional activities, providing insights into the nature of their income generation.

2.) Tax Residence and Certificates: Documentation confirming the client's tax residence and relevant tax certificates.

3.) Income Details: Information regarding the amount and source of the client's income, which may include income tax returns and salary slips.

4.) Asset Composition: Documentation highlighting the composition and extent of the client's assets, such as property deeds, statements of securities portfolios, life insurance policies, or proof of inheritance.

SUNMONEY SOLAR GROUP assured that the collection and storage of this information will be handled with utmost care and in strict accordance with data protection and privacy regulations. We prioritize the confidentiality and security of your personal and financial data.

However, it is essential to note that if an applicant or client refuses to cooperate with the request for source of funds documentation, SUNMONEY SOLAR GROUP will unable to proceed with transactions on their behalf. Consequently, the application process or client relationship will be terminated, and any funds associated with the client will be promptly returned.

3.1.5 Politically Exposed Person

A PEP is defined as a natural person who currently holds, or has held within the last 12 months, a high-ranking public office position. Due to their proximity to governmental and/or organizational funds, PEPs are considered high-risk individuals who may potentially abuse their position of power by accepting bribes or embezzling public funds. This classification also extends to the immediate family members of PEPs and individuals with close business ties to them. To address the risks associated with PEPs, our company employs rigorous checks.

PEPs are considered high-risk clients due to the following factors:

1.) Authority and Proximity to Funds: PEPs have the potential to misappropriate funds and attempt to launder them, given their authority and close association with governmental and/or organizational finances.

2.) Susceptibility to Bribery and Corruption: PEPs may be vulnerable to bribery and corruption due to their influential positions.

3.) Control over Business Operations: Within businesses, PEPs may hold positions that grant them

authority over company operations, which increases the risk of misuse or fraudulent activities.

4.) Access to State Assets and Concealment: PEPs may have access to state assets and possess the Power to implement measures that hinder the detection of money laundering or terrorist financing activities.

SUNMONEY SOLAR GROUP takes reasonable measures to determine whether an applicant, client, or beneficial owner qualifies as a PEP or an individual entrusted with a prominent function by an international organization. This involves regular screening of clients against national and international PEP/Sanctions lists.

If a positive match is found during the screening process, additional measures are undertaken. The client is requested to provide Proof of Address (POA) and Proof of Source of Funds (PSOF) and a report to the FIU must be filled. Furthermore, the acceptance of a PEP as a client requires approval from the appropriate authority within our organization. For existing clients who are subsequently identified as matching a PEP list, the same actions are taken.

By adhering to these risk mitigation measures, SUNMONEY SOLAR GROUP ensure compliance with regulatory guidelines and maintain the highest level of transparency and integrity in our operations. SUNMONEY SOLAR GROUP commitment to the prevention of money laundering and terrorist financing activities is of paramount importance.

3.1.6 FATF Travel Rule

Virtual asset service providers (VASPs), which include cryptocurrency exchanges and custodial wallets, are required to collect and transmit specific customer information during cryptocurrency transactions. This regulation aims to enhance the transparency and traceability of digital asset transactions in order to combat money laundering, terrorist financing, and other illicit activities.

The information that VASPs are expected to collect and transmit typically includes:

1.) Originator Information: This includes the name and virtual asset wallet address of the person initiating the transaction. VASPs must verify the identity of the originator through appropriate know-your-customer (KYC) procedures.

2.) Beneficiary Information: VASPs are also required to collect and transmit the name and virtual asset wallet address of the beneficiary or recipient of the transaction.

3.) Transaction Details: Relevant details of the transaction, such as the amount and date of the transfer, should be included in the transmission.

The purpose of collecting and transmitting this information is to enable effective and efficient cross-border exchange of information between VASPs. It allows the identification and monitoring of potentially suspicious or illicit transactions.

It's important to note that the specific implementation and requirements of the FATF Travel Rule may vary between jurisdictions. Each country is responsible for incorporating the rule into their local regulatory frameworks and ensuring compliance within their respective jurisdictions.

Crypto service providers, including exchanges and custodial wallets, should familiarize themselves with the regulations set forth by their local regulatory authorities to ensure compliance with the FATF Travel Rule and other relevant requirements.

3.2 New Technologies

The Company identifies and assesses the money laundering or terrorist financing risk that may arise in the relation to:

a) the development of new products and new business practices, including new delivery mechanisms, and
b) the use of new or developing technologies for both new and pre-existing products.

The risk assessment takes place prior to the launch of new products, business practices or the use of new or developing technologies. Appropriate measures are taken to manage and mitigate those risks.

The Company does not deal with technologies offering anonymity or with anonymity-enhanced transactions.

3.3 Reliance on third parties

The Company may rely on third parties if:

- The Company immediately obtains the necessary information of the CDD measures from the third party.
- The Company takes adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay
- The Company checks that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements
- When determining in which countries the third party that meets the conditions can be based, the Company should have regard to information available on the level of country risk

The Company can rely on a third party to perform some or all of the following elements of the CDD process:

a) identifying the client
b) verifying the client identity, and
c) gathering information on the purpose and intended nature of the business relationship
d) Conducting on going due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institutions knowledge of the customer, their business and risk profile, including where necessary .

The Company shall take steps to ensure that third parties performing CDD measures have policies that are consistent with the Company AML/CFT Policy. In order to check how the CDD related services of third parties comply with the AML/CFT regulations, the Company sends them an email periodically (annually) with the request to explain how they make sure that their services comply with the AML/CFT regulations. Additionally, the Company requests what policies they have put in place to make sure that they comply with the AML/CFT regulations and the Company's own internal policies.

3.4 Sanctions

The Company screens its applicants during onboarding and its clients on a regular basis against sanctions.
The Company screens the applicant / client's first name, last name and/or birthdate against Sanction lists. When there is a hit the customer support team performs the first manual check to see if there is

a potential positive hit. When a potential positive hit is detected, this is immediately reported to the CO.

If a positive hit is a result from the screening against the sanctions lists:

1) funds and / or economic resources are directly frozen. preventing the funds and / or economic resources from being made available directly or indirectly and prevent banned financial services from being provided

2) The CO reports the "freezing" immediately to the FIU or when required to another local competent authority.
3) Any questions the FIU asks as a result of the report are answered immediately by the CO.
4) If the "hit" can be classified as an unusual transaction, this is also reported to the FIU.

The Company does not accept applicants on sanctions lists as clients. When an applicant has a positive hit on the sanctions lists the onboarding process is stopped. In case a hit has been identified for an existing client relationship, the account will be disabled before the termination of the client relationship. To prevent tipping off the reason communicated to the Client will be, "because of compliance reasons".

The Compliance/MLRO will strive to file an external FIU via the GoAML platform within 24 hours of determination or as soon as reasonably possible, whichever is earlier. There may be circumstances in which an SAR needs to be filed on an urgent basis – these will be considered and the MLRO will strive to file the report at the earliest possible in such cases, in line with legal and regulatory requirements. Any request received from the authority for additional information/documents via the GoAML platform will be actioned by the MLRO promptly, without delay and in line with legal requirements and guidance. All decisions to file or not file a SAR will be signed-off by the MLRO.

Adequate guidance on filing SARs via the GoAML platform have been published by the UAE authorities, and shall be referred to and complied with by the MLRO at all times. Recent guidance published can be accessed here:

- https://www.uaefiu.gov.ae/en/more/knowledge-centre/system-guides.

False positive: If the processing of the alert leads to the conclusion that the Client who is the subject of the alert is not the person designated by a freezing measure, the alert can be lifted and there is no need to freeze the assets.

Vigilance in doubt of a positive hit: If the evidence does not allow the freezing measure to be validated comfortably, the vigilance will be adapted accordingly and will move to the complementary level.

As soon as a freezing measure is lifted, the Company lifts all restrictions implemented, without waiting for confirmation from the FIU or other local competent authority. The client's risk classification will be reviewed accordingly.

The different regimes in force will be applied:

- The regimes resulting from United Nations Security Council resolutions
- The regimes resulting from CFSP decisions of the Council of the European Union
- OFAC list
- The national regime of asset freezing

3.5 Country Risk

A trustful source of high-risk countries are as follows in the FATF lists.

These lists are available here: http://www.fatf-gafi.org/countries/#high-risk.

3.6 Transaction Monitoring (TM)

3.6.1 Suspicious and unusual transactions and activity

Where the Company knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing, the Company is required to report to the FIU the following indicators that could indicate an unusual or suspicious transaction when:

The following circumstances serve as indicators for reporting unusual or suspicious transactions, regardless of the amount involved:

1.) Transactions Related to Money Laundering or Terrorist Financing: Any transaction that gives us reasonable grounds to believe it may be associated with money laundering or terrorist financing activities should be reported to the FIU.

2.) Transactions Involving AED [amount] or More: Transaction's meeting or exceeding the specified threshold of AED [amount] should also be reported to the FIU.

The below examples illustrate further circumstances that may indicate a suspicious or unusual transaction:

- Unusual Size, Nature, or Frequency: Transactions or orders to trade that deviate significantly from a client's typical patterns in terms of size, nature, or frequency.
- Unclear Identity of the Transacting Party: Situations where it is difficult to ascertain the true identity of the individual behind a transaction.
- Unclear, Unusual, or Inexplicable Source of Funds: Instances where the source of funds appears unclear, unusual, or lacks a reasonable explanation.
- Refusal to Provide Details on Source of Funds: Clients who refuse to provide elaboration or clarification regarding the origin of their funds.
- Incomplete or Inconsistent Information: Instances where the provided information is incomplete or exhibits inconsistencies.
- Negative Press or Information: The presence of negative press or information that could potentially indicate suspicious activity.

During the client onboarding process, Customer Due Diligence (CDD) is diligently conducted for all applicants. However, in cases where we were unable to obtain the required client information during the CDD process and there are indications of potential involvement in money laundering or terrorist financing, we promptly report such cases to the FIU, along with a detailed explanation of the reasons for the failure to complete client due diligence.

SUNMONEY SOLAR GROUP is aware that all suspicious or unusual transactions, including attempted and intended transactions, are reported to the FIU by the designated Compliance Officer (CO). We operate with utmost transparency and adhere to strict reporting protocols to ensure the integrity of our operations and contribute to the prevention of financial crimes.

3.6.2 Screening of Crypto Asset Transactions

As part of SUNMONEY SOLAR GROUP commitment to regulatory compliance and risk mitigation, SUNMONEY SOLAR GROUP shall implement a system to monitor transactions.

The system shall be deployed to conduct ongoing monitoring and risk assessment of all incoming and outgoing crypto asset transactions. It analyzes various factors associated with the transactions to assign a risk score. The risk factors taken into consideration include but are not limited to Gambling, Illegal Services, Miner, Mixing Services, Online Marketplaces, Online Wallets, P2P Exchanges with High ML Risks, P2P Exchanges with Low ML Risks, Payment Processors, Ransoms, Scams, Stolen Coins, ATM, Darknet Marketplaces, Darknet Services, Exchange with High ML Risk, Exchange with Low ML Risk, Exchange with Moderate ML Risk, Exchange with Very High ML Risk, Fraudulent Exchange, and Others.

SUNMONEY SOLAR GROUP screening process distinguishes between incoming and outgoing transactions, and each transaction is assigned a risk level based on its score.

We have established the following risk levels and corresponding actions for outgoing transactions:

1.) 0-40% Risk Score;

- No action is required as these transactions are considered low risk.

2.) 41%-60% Risk Score (manual involvement):

- The Company will conduct a comprehensive analysis of the client and the transaction.
- We may request the client to provide additional information and confirm the origin of funds as well as the destination of the crypto assets.
- If we determine that the risk can be adequately mitigated, we will proceed with the transaction and continue working with the client.

3.) 61-100% Risk Score (manual involvement):

- The Company will undertake Enhanced Due Diligence (EDD) measures, which may involve gathering additional information and conducting further analysis.
- If deemed necessary, we will submit a Suspicious Activity Report (SAR) to the Financial Intelligence Unit (FIU) in accordance with our regulatory obligations.

Incoming transactions:

1.) 0-30% Risk Score:

- No action is required for these low-risk transactions.

2.) 31%-50% Risk Score (manual involvement):

- We perform a comprehensive analysis of the client and the transaction.
- We may request you to confirm the origin of funds and provide details of the source account from which the funds were transferred to your account on our platform.
- If we determine that the risk can be adequately mitigated, we will proceed with the transaction and continue our relationship with you.

3.) 51-100% Risk Score (manual involvement):

- We undertake Enhanced Due Diligence (EDD) measures, which may involve gathering additional information and conducting further analysis.

- If necessary, we will submit a Suspicious Activity Report (SAR) to the FIU as required by our regulatory obligations.

SUNMONEY SOLAR GROUP is aware that it is important that there are exceptions to the risk levels outlined above. In cases where the risk category exceeds 5% for indicators marked as "Danger" according to the results provided by the monitoring system, and considering the amount of crypto assets involved, we will not provide services to clients. In such instances, we will consider submitting a Suspicious Activity Report (SAR) to the FIU. The indicators marked as "Danger" include but are not limited to Illegal Services, Darknet Marketplaces, Darknet Services, Mixing Services, Sanctions, Ransoms, Scams, Stolen Coins, and Fraudulent Exchange.

SUNMONEY SOLAR GROUP is also aware that if a transaction falls into this exceptional category, both your wallet and your account with us will be temporarily frozen until further instructions are received from the Compliance Officer (CO) or the FIU.

3.6.3 System and Controls

SUNMONEY SOLAR GROUP have implemented to detect and address any unusual or suspicious transactions within our organization.

SUNMONEY SOLAR GROUP prioritize the detection of irregular behaviour and employ an automated surveillance system to continuously monitor and analyse all transactions conducted on our platform. This includes monitoring every transaction executed, as well as every order placed, modified, cancelled, or rejected.
Our surveillance system is designed to identify any transactions or orders that deviate from the expected patterns, enabling us to promptly identify and investigate potential irregularities.
By leveraging advanced technology and data analysis techniques, we aim to enhance our ability to detect and mitigate any suspicious activities.

Furthermore, SUNMONEY SOLAR GROUP has implemented comprehensive review processes that enable us to closely examine clients who exhibit irregular behaviour or engage in transactions that raise concerns. These reviews are conducted to ensure compliance with regulatory requirements and to prevent any potential illicit activities such as money laundering or terrorist financing.

Our systems and controls are regularly assessed and updated to align with industry best practices and regulatory guidelines.

4	Risk Classification

4.1 Risk Classification Process

SUNMONEY SOLAR GROUP follows a comprehensive risk classification process to assess the level of risk associated with each client. Below is a step-by-step overview of our risk classification process:

1.) Identification and Verification: All clients are required to undergo a thorough identification and verification process to establish their identity.

2.) Client Risk Assessment (CRA): During the CRA, the Company collects information about the client and considers any known risk indicators (KYC information). The gathered information must be sufficient to identify potential money laundering (ML) and terrorist financing (FT) risks associated with the client.

3.) Sanctions Checks: Ongoing sanctions checks are conducted, and clients are screened against sanction lists. If a client is identified as a true match on the sanction list, they are classified as a Severe risk and will not be accepted as a client.

4.) Politically Exposed Persons (PEP) Checks: Ongoing PEP checks are performed, and clients are screened against PEP lists. If a client is identified as a PEP, they are classified as a High risk. To continue with the onboarding process, the client is required to provide Proof of Address (POA) and Proof of Source of Funds (PSOF). Existing clients who are identified as PEPs are also required to provide POA and PSOF to continue making deposits, withdrawals, and trades. Failure to provide the required documentation will result in no transactions being allowed on the platform.

5.) Deposit Size Risk Check: After the CRA, a deposit size risk check is conducted. If a client makes a deposit of a specified amount or more (e.g., xx EUR), they are classified as a High risk. To continue trading on the platform, the client is required to provide POA and PSOF.

6.) Risk Categorization: Based on the gathered information and the results of the above checks, the client is categorized as Medium, High, or Severe risk. The client's risk profile is determined during the client risk assessment process (refer to section 5.3). Enhanced Due Diligence (EDD) is required for clients classified as High risk, and they are asked to provide POA and PSOF.

By following this risk classification process, SUNMONEY SOLAR GROUP ensure that appropriate measures are taken to address the risk level associated with each client and comply with regulatory requirements.

4.2 Risk Mitigation

4.2.1 Risk profile

To mitigate risks associated with clients, the Company implements the following risk profile measures:

1.) Risk Profile Requirement: The Company ensures that every client undergoes a risk profile assessment during the onboarding process. This assessment helps determine the level of risk associated with each client.

2.) Risk Profile Levels: The Company categorizes clients into three risk profile levels: Medium, High, and Severe. The categorization is based on various factors, including the client's country of residence, country of nationality, sources of funds, and the results of the client risk assessment (CRA).

a. Medium Risk: Clients in this category are deemed to have a higher-than-average risk level to the Company. The risk level depends on factors such as the client's country of residence, country of nationality, sources of funds, and the results of the CRA.

b. High Risk: Clients are classified as high risk under the following circumstances: Politically Exposed Persons (PEPs) Residents of high-risk jurisdictions, Clients depositing a total amount exceeding 3,500 AED into their accounts as per FATF recommendations, Clients identified as high risk for other reasons, subject to the decision of relevant personnel.

c. Severe Risk: Clients categorized as severe risk are considered unacceptable If an existing client's risk profile changes to severe, the client will be offboarded.

By implementing risk profile ratings, the Company effectively assesses and addresses the level of risk associated with each client. This helps ensure compliance with regulatory requirements **and allows for appropriate risk mitigation measures to be applied.**

4.3 Severe Risks

Some Client takes significant measures to identify and mitigate severe risks associated with applicants and clients. The following scenarios are considered severe risks, and applicants or clients falling into

these categories will not be accepted or, in the case of existing clients, the business relationship will be terminated:

1.) Presence on Sanction Lists: Applicants or clients found on the "consolidated list of persons, groups and entities subject to EU financial sanctions," the UN-sanction list, OFAC sanction list, or any national sanction list are considered severe risks.

2.) Involvement with Criminal Organizations: Applicants or clients suspected to be involved with a criminal organization pose a severe risk.

3.) Involvement in Criminal Activity: Applicants or clients suspected of engaging in criminal activities, such as fraud, present a severe risk.

4.) Anonymity and False Identity: Applicants or clients who seek anonymity or provide false identity documents are considered severe risks.

5.) Refusal to Provide Required Information or Documents: Applicants or clients who refuse to provide the necessary information or documents pose a severe risk.

6.) US-Person Status: Applicants or clients identified as US-Persons are considered severe risks.

7.) Funds Related to Sanctions: Applicants or clients whose funds are identified as related to sanctions are classified as severe risks.

These measures are in place to ensure SUNMONEY SOLAR GROUP compliance with regulations, safeguard its reputation, and maintain a secure environment for all clients. By strictly identifying and addressing severe risks, the Company upholds its commitment to risk mitigation and compliance with applicable laws and regulations.

4.4 Client Risk Assessment

SUNMONEY SOLAR GROUP places great importance on conducting a thorough Client Risk Assessment (CRA) to evaluate the level of risk associated with each applicant in terms of financial crime. The CRA allows for the differentiation of clients based on their risk profile, enabling the implementation of appropriate Customer Due Diligence (CDD) and ongoing monitoring procedures. It is essential to tailor these procedures according to the specific risk posed by each client, taking into account factors such as their country of origin.

The Company employs various measures for the Client Risk Assessment, including but not limited to the following:

1.) Strict Onboarding Procedures: All clients undergo the same rigorous onboarding procedures to ensure consistent compliance standards.

2.) Additional Identity Verification: Verification of additional aspects of the client's identity is performed to enhance the accuracy and reliability of client information.

3.) Account Holder Verification: Verification is conducted to ensure that client deposits for fiat transactions originate from the named account holder.

4.) Ongoing Monitoring of Crypto Asset Wallets: High-risk activity in crypto asset wallets is continuously monitored, enabling the detection of suspicious transactions.

5.) Verified Communication: Communication with clients is conducted through verified email addresses to establish secure and authenticated channels of communication.

6.) Source of Funds Inquiry: Clients may be questioned about the source of funds used in their transactions, and in some cases, a valid proof of the source of funds may be requested.

In addition to the above measures, the CRA goes further by subjecting clients to more stringent requirements and utilizing additional mechanisms, including but not limited to:

1.) Adverse Media Screening: Clients undergo adverse media screening (ZZZ) to identify any negative news or information associated with them.

2.) Enhanced Cryptocurrency Investigation: SUNMONEY SOLAR GROUP conduct enhanced investigations into cryptocurrency transactions, providing an extra layer of scrutiny to mitigate risks.

By implementing these measures and conducting a comprehensive CRA, SUNMONEY SOLAR GROUP aims to effectively assess and manage the risks posed by its clients. This ensures compliance with regulations, minimizes the potential for financial crimes, and upholds the integrity and reputation of the Company and its services.

5 Monitoring

5.1 Monitoring Procedure

SUNMONEY SOLAR GROUP recognize the importance of ongoing monitoring to ensure the accuracy and currency of client information. As part of SUNMONEY SOLAR GROUP commitment to regulatory compliance and risk management, we conduct continuous monitoring throughout the business relationship to ensure that client transactions align with the knowledge we have of the client and their established risk profile.

The ongoing due diligence process involves regularly reviewing client activity and comparing it against the client's known risk profile. This allows us to detect any inconsistencies or unusual patterns that may indicate potential financial crime or changes in the client's risk profile. By performing ongoing due diligence, we aim to maintain the integrity of our services and promptly address any emerging risks.

During the ongoing monitoring process, we may:

1.) Review Transaction Activity: We analyse client transactions, including deposits, withdrawals, and trades, to identify any unusual or suspicious patterns that deviate from the client's expected behaviour.

2.) Update Client Information: We periodically request clients to provide updated information, such as changes in their personal details, source of funds, or business activities, to ensure the accuracy and completeness of their profiles.

3.) Reassess Risk Profile: If significant changes are identified in the client's transactional behaviour or other relevant factors, we may reassess the client's risk profile to determine if any adjustments or enhanced due diligence measures are necessary.

4.) Conduct Enhanced Due Diligence (EDD): In certain circumstances, where the client's activities or risk level warrant further scrutiny, we may initiate EDD procedures to gather additional information and mitigate potential risks.

By actively monitoring and conducting ongoing due diligence, we aim to stay vigilant against financial crime, including money laundering, terrorist financing, and other illicit activities. Our commitment to ongoing monitoring enables us to fulfil our regulatory obligations, protect our clients and the integrity of our services, and contribute to the overall security and stability of the financial system.

5.2 Periodic Review (PR)

The Periodic Review is an essential component of our risk management framework to ensure the ongoing appropriateness of our client relationships. The frequency of the review is determined based on the risk profile assigned to each client.

The monitoring frequency for each risk profile is as follows:

Medium Risk	Once every two years
High Risk	Once a year
Severe Risk:	Unacceptable as a client

During the Periodic Review, the client is required to undergo a comprehensive assessment of their risk profile. This assessment aims to identify any changes or developments that may have an impact on the client's current risk profile. It involves a review of various elements, including but not limited to:

1.) Client Information: The client's personal and business information is reviewed to ensure its accuracy and relevance. This includes details such as identification documents, contact information, and any updates to their profile.

2.) Source of Funds: The client is requested to provide updated information regarding the source of their funds. This is crucial to assess the legitimacy and legality of their financial resources.

3.) Transaction Activity: A thorough analysis of the client's transaction history is conducted to identify any unusual or suspicious patterns that may indicate potential financial crime.

4.) Risk Factors: The client's risk profile is reassessed based on their current circumstances, such as changes in their business activities, geographic location, or other relevant factors.

The Periodic Review helps us ensure that our risk management measures remain aligned with the evolving nature of financial crime and regulatory requirements. It enables us to promptly identify and address any potential risks associated with our client relationships.

If significant changes are identified during the Periodic Review that may impact the client's risk profile, appropriate measures will be taken, including conducting enhanced due diligence or reclassifying the client's risk profile accordingly.

5.3 Event Driven Review

An event driven review is a critical component of our ongoing due diligence process. It is triggered by significant changes or material information that may impact the client's risk profile, requiring a thorough reassessment of their relationship with our company. This review aims to ensure that our risk management measures remain up to date and aligned with the evolving risk landscape.

The following are some examples of events that may trigger an event driven review, although this list is not exhaustive:

1.) Adverse Media: The client is identified in negative news reports, media coverage, or other publicly available information that raises concerns about their reputation or involvement in illicit activities.

2.) Relocation: The client moves to another country, which may introduce new risks or necessitate compliance with different regulatory frameworks.

3.) PEP/Sanction List Hit: The client is identified as a politically exposed person (PEP) or matches an entry on any sanction list, indicating a higher risk of potential financial crime.

4.) Deposit Size: The client makes a significant deposit that exceeds predetermined thresholds, which may require enhanced due diligence to ascertain the legitimacy of the funds and the client's financial activities.

5.) Unusual Transactions: The client engages in transactions that are unusual in terms of size, frequency, nature, or patterns, indicating potential suspicious activity or money laundering.

When an event driven review is triggered, a comprehensive due diligence review is conducted to reassess the client's risk profile. This may involve requesting updated information, conducting additional background checks, and analysing the impact of the event on the client's risk profile.

Based on the outcome of the event driven review, appropriate risk mitigation measures will be implemented, such as adjusting the risk rating, conducting enhanced due diligence, or terminating the business relationship if necessary.

5.4 Crypto Transaction Monitoring

SUNMONEY SOLAR GROUP has a comprehensive system for monitoring crypto asset transactions. This monitoring system is designed to detect and prevent suspicious activities, money laundering, and other illicit financial transactions.

Key features of our Crypto Transaction Monitoring system include:

1.) Real-time Transaction Monitoring: Our system continuously analyzes and reviews all incoming and outgoing crypto asset transactions in real-time. This allows us to promptly identify any unusual or suspicious activities that may require further investigation.

2.) Risk-based Scoring: Each transaction is assigned a risk score based on various factors, such as transaction amount, frequency, counterparties involved, and historical patterns. This risk score helps prioritize transactions for further analysis based on their potential for illicit activities.

3.) Rule-based Alerting: Our monitoring system is configured with predefined rules and thresholds that trigger alerts for specific types of suspicious transactions. These rules are designed to capture known patterns of illicit behaviour, such as structuring transactions, high-volume transfers, or involvement with sanctioned entities.

4.) KYT (Know Your Transaction): We utilize KYT services to perform transaction screening against known risk indicators, including darknet marketplaces, sanctions lists, stolen coins, and other high-risk categories. This enables us to identify transactions associated with illicit activities or entities of concern.

5.) Enhanced Due Diligence (EDD): In cases where a transaction or account raises concerns or meets certain risk criteria, our compliance team conducts additional investigations and due diligence. This may involve requesting further information from the client, verifying the source of funds, or conducting more extensive background checks.

6.) Suspicious Activity Reporting: If our monitoring system detects any transactions that are deemed suspicious or indicative of illicit activity, we promptly report them to the appropriate authorities, such as the Financial Intelligence Unit (FIU), as required by applicable regulations and laws.

SUNMONEY SOLAR GROUP Transaction Monitoring system is continuously updated and refined to stay ahead of evolving risks and emerging trends in the crypto asset space. We remain committed to maintaining a secure and compliant environment for our clients, ensuring the integrity of our platform and protecting against financial crime risks.

6	Reporting

6.1 Reporting

SUNMONEY SOLAR GROUP prioritize compliance with regulatory requirements and have established procedures for reporting suspicious activities to the Financial Intelligence Unit (FIU). The FIU is the designated government agency responsible for receiving, analysing, and disseminating financial intelligence related to potential money laundering, terrorist financing, and other illicit activities.

Key aspects of our reporting process and engagement with the FIU include:

1.) Suspicions and Red Flags: Our systems and controls are designed to identify and assess suspicious transactions or activities. We have implemented measures to detect red flags that may indicate potential money laundering or terrorist financing, such as unusual transaction patterns, high-risk jurisdictions, and unexplained sources of funds. Whenever such suspicions arise, we immediately initiate the reporting process.

2.) Non-Disclosure of Suspicion: It is essential to maintain the integrity of the investigation and prevent potential interference or tipping off of individuals involved. Therefore, our policy strictly prohibits informing the client or any third party that a suspicious activity report is being filed or that an investigation is underway. This ensures the confidentiality of the reporting process and enhances the effectiveness of subsequent actions taken by the relevant authorities.

3.) Reporting Responsibilities: The responsibility for reporting suspicious transactions to the FIU lies with the Chief Officer (CO) or the designated responsible party within our organization. The CO ensures that all necessary information is included in the report and that it is promptly submitted to the FIU in accordance with regulatory requirements.

4.) Compliance with Regulatory Obligations: We are committed to complying with all applicable laws and regulations related to reporting suspicious activities to the FIU. Our compliance team regularly reviews the adequacy of our reporting systems and procedures to ensure that they remain effective and in line with regulatory expectations.

5.) Ongoing Assessment: We periodically assess the adequacy and effectiveness of our systems for identifying and reporting suspicious transactions. This includes reviewing and updating our internal controls, training programs, and monitoring mechanisms to address emerging risks and industry best practices.

It's important to note that the exact reporting obligations and procedures can vary significantly depending on the jurisdiction and the specific regulatory framework governing cryptocurrencies. Therefore, it is essential for SUNMONEY SOLAR GROUP to understand and comply with the reporting requirements established by the relevant authorities in their jurisdiction.

6.2 Tipping Off

The principle of non-disclosure, commonly known as "tipping off," is a fundamental aspect of reporting suspicious transactions and maintaining the integrity of the investigation. Here's a summary of the key points related to tipping off:

1.) Tipping Off Prohibition: The Company must not inform the client or any other individuals that suspicions have been raised or that an investigation is underway. Informing the client about these matters is considered tipping off, and it is a criminal offense in most jurisdictions. The objective is to prevent potential criminals from becoming aware of the investigation and taking steps to evade detection.

2.) Information that Should Not be Disclosed: The following information should not be disclosed to the client or any other party:

a. The fact that a report of a suspicious or unusual transaction is being, will be, or has been submitted.
b. The fact that the Financial Intelligence Unit (FIU) has requested additional information.
c. The fact that a money laundering or terrorist financing analysis is being or may be carried out.
d. Any discussions held to determine whether a suspicious or unusual transaction should be reported.

3.) Confidentiality of the Report to the FIU: The report on a suspicious or unusual transaction submitted to the FIU must be treated with utmost confidentiality. It is strictly forbidden to disclose the existence and content of the report to clients, the owner of the money, the originator of the transactions, or any third parties, except for authorized individuals within the Company such as supervisory authorities, the Compliance Officer (CO), Head of Compliance, top management, and other designated personnel.

4.) Disclosure within the Company: The report submitted to the FIU should be disclosed within the Company as necessary, unless decided otherwise by the FIU. This means that individuals with a legitimate need-to-know within the Company, particularly those responsible for compliance and oversight, may have access to the report to ensure proper handling and follow-up.

5.) Breach of Confidentiality: Breaching the confidentiality of a report to the FIU is a serious matter. If an individual within the Company fails to comply with the obligation of confidentiality, they may be subject to fines and other legal consequences.

SUNMONEY SOLAR GROUP is aware of the strict rules regarding tipping off and to strictly adhere to confidentiality obligations. By maintaining confidentiality, the integrity of the investigation is preserved, allowing the FIU to conduct their analysis effectively and take appropriate actions to combat money laundering and terrorist financing activities.

6.3 Timing of Reports

Upon suspicion or reasonable grounds to suspect that the proceeds of a crypto transaction are related to a crime or the intention to use funds for criminal activities, the Compliance Officer (CO) shall be responsible for:

1.) Prompt Reporting: The CO must immediately report the suspicious transaction or activity to the appropriate regulatory authorities, such as the Financial Intelligence Unit (FIU), in accordance with the applicable crypto regulations. The report should include all relevant details and supporting documentation.

2.) Timely Investigation: The CO should initiate an internal investigation to gather additional information and evidence related to the suspicious transaction. The investigation should be conducted promptly and diligently to determine the nature and extent of the suspected illegal activity.

3.) Risk Assessment: The CO, in collaboration with relevant personnel and legal advisors, if necessary, should assess the risks associated with the suspicious transaction and evaluate its potential impact on the company's compliance with crypto regulations. This assessment will help determine the appropriate course of action.

4.) Documentation and Record-Keeping: The CO must ensure that all relevant information, including the suspicion report, supporting documentation, investigation findings, and any

subsequent actions taken, are properly documented and maintained. This documentation is crucial for compliance purposes and potential future audits or investigations.

5.) Non-Disclosure: The CO must strictly adhere to the principle of non-disclosure, also known as "tipping off." It is prohibited to inform the client or any third parties that a suspicious activity report has been filed or that an investigation is underway. Any breach of this confidentiality obligation may result in legal consequences.

The timing of reporting is critical in crypto regulations, and it is essential for the CO to act swiftly and responsibly when suspicions arise. By promptly reporting and investigating suspicious transactions, the CO plays a vital role in preventing money laundering, terrorist financing, and other illicit activities within the crypto space.

All reports regarding Suspicious Transactions in the UAE shall be made as follows:

a. Reporting to the UAE FIU and VARA: The reports must be submitted to the UAE Financial Intelligence Unit (FIU) and the Virtual Asset Regulatory Authority (VARA) through the designated **GoAML platform** or any other approved means specified by the UAE FIU and/or VARA. This ensures that the relevant authorities receive the necessary information to investigate and take appropriate actions.

b. Compliance with VARA Guidance: The reporting of Suspicious Transactions should be done in accordance with any guidance or instructions issued by VARA. VARA may provide specific guidelines, templates, or reporting formats to be followed when submitting the reports. It is important for the reporting entity to stay updated with the latest guidance issued by VARA to ensure compliance with the reporting requirements.

By adhering to these reporting procedures and following the guidelines set by VARA, the reporting entity can fulfill its obligations and contribute to the efforts in combatting money laundering, terrorist financing, and other illicit activities within the UAE's virtual asset sector.

6.4 How to report and the content of the reports

When reporting suspicious or unusual transactions, the following procedures and information should be taken into account:

1.) Blocking Transactions: Upon identifying an atypical or suspicious transaction, it is generally advisable to block the transaction to allow for investigations and the preparation of reports before proceeding further. This allows the Financial Intelligence Unit (FIU) to exercise its right to oppose the transaction if necessary.

2.) Exceptional Reporting: In exceptional cases where it is not possible to suspend the execution of the transaction or if postponing it could hinder ongoing investigations, the suspicion report should be made promptly, even if it is submitted after the transaction has been carried out.

3.) Role of the FIU Reporter (CO): The designated FIU reporter, typically the Compliance Officer (CO), is responsible for processing alerts, conducting investigations, and gathering relevant information for reporting purposes. This includes reviewing the client's transaction history, researching crypto transactions related to the portfolios under investigation, identifying the parties involved, cross-referencing supporting documents in the client file, and examining the reputation of the client and other parties involved.

4.) Comprehensive Understanding: It is important for the CO to undertake all reasonable steps to gain a proper understanding of the transaction before submitting a suspicious transaction

report. This ensures that the report is based on sufficient information and supporting evidence.

5.) Content of Suspicious Transaction Reports: The reports submitted to the FIU should include, at a minimum, the following information:

- Identity: The identity of the client, including their profession if applicable, and the identity of any person on whose behalf the transaction is intended or has been conducted.
- Identification Documents: The type and number of the document(s) used to identify the client and any other relevant individuals involved in the transaction.
- Transaction Details: The type of transaction, along with the time and place where it took place.
- Funds and Values: The amount, allocation, and source of funds or other values associated with the transaction.
- Reasons for Suspicion: A clear explanation of the reasons and circumstances that lead to the conclusion that the transaction is considered suspicious or unusual.

6.) Additional Information Requests: After the initial report submission, the FIU may request additional information pertaining to the reported transaction. In such cases, the requested information should be provided promptly and in writing, unless emergency situations require immediate verbal communication.

By following these reporting procedures and providing the necessary details, the reporting entity can ensure compliance with regulatory requirements and assist the FIU in its efforts to combat money laundering, terrorist financing, and other illicit activities.

6.5 Documentation and record keeping

The documentation and record-keeping requirements for suspicious transaction reports are as follows:

1.) Storage of Reports: The suspicious transaction reports submitted to the FIU should be kept in a secure location that is accessible only to the designated FIU reporter or correspondent, typically the Compliance Officer (CO). This ensures the confidentiality and integrity of the reports.

2.) Retention Period: The following documents related to suspicious transaction reports must be retained for a period of five years:

3.) Copy of Suspicious Transaction Report: A copy of the suspicious transaction report that was transmitted to the FIU should be kept. This includes all relevant information and details provided in the report.

4.) Supporting Documents: Any documents that were transmitted along with the suspicious transaction report should also be retained. These documents may include additional evidence, transaction records, identification documents, or any other relevant information that was deemed necessary to support the report.

5.) Acknowledgment of Receipt: If applicable, an acknowledgment of receipt of the suspicious transaction report from the FIU should be retained as part of the documentation.

By maintaining these records for the required period, the reporting entity demonstrates compliance with regulatory obligations and ensures the availability of relevant information for potential investigations or audits in the future

7	Internal Controls

7.1 Controls of clients file & throughout the Business Relationship

The controls of client files and follow-up processes in relation to AML/CFT (Anti-Money Laundering and Countering the Financing of Terrorism) measures include the following levels and activities:

Level 1: At each relationship entry and throughout the business relationship

- Customer risk profiling: Conducting an initial assessment of the client's risk profile based on factors such as country of residence, nationality, sources of funds, and other relevant information.
- Automated screening: Implementing automated screening processes, including daily monitoring, to identify any potential red flags or suspicious activity.
- Consistency check: Ensuring consistency and compliance with internal compliance standards and regulations.
- Validation of KYC file: Verifying that the client's KYC (Know Your Customer) file is complete and contains all the necessary information and documents based on the risk profile.
- Updating client files: Regularly updating client files to reflect any changes in the client's risk profile or regulatory requirements. This includes updating systems to accommodate legislative and regulatory changes.

Level 2: Annual control by sampling (CO)

- Completeness of client files: Conducting periodic checks to ensure that client files are complete and contain all the required information and documents based on the risk profile and account activity.
- Compliance with internal norms: Verifying that client files comply with internal normative developments and standards.
- Validation of KYC files: Assessing the level of validation and accuracy of the KYC files.
- Updating client files: Updating client files at predetermined frequencies to ensure they remain current and accurate.

Transaction supervision controls:

Level 1: Ongoing basis (software, operational, or CO)

- Identification of atypical transactions: Implementing measures to identify transactions that deviate from normal patterns or show suspicious characteristics.
- Alert notification: Notifying operational staff of identified alerts for further investigation and processing.
- Escalation process: Establishing a process for escalating suspicious transactions or high-risk activities to appropriate personnel for further action.

Level 2: Quarterly control by sampling (CO)

- Completeness of alert processing: Checking the completeness of processing alerts raised in Level 1.

- Analysis of alerts: Conducting sample analysis of alerts generated to verify their effective processing.
- Control for high-risk clients: Monitoring and strengthening monitoring for clients who have been the subject of a suspicious transaction report.

Controls relating to screening:

Level 1: On an ongoing basis

- Automated screening: Conducting automated screening processes, such as identifying Politically Exposed Persons (PEPs) and checking against sanction lists, during the onboarding process.
- Daily screening: Implementing daily automated screening of the client base to identify any new matches against PEP or sanction lists.
- Screening alert handling process: Establishing a process for handling screening alerts and conducting further investigations when necessary.

Level 2: Annually

- Completeness check of screening alert processing: Checking the completeness of processing screening alerts.
- Sample analysis of processed screening alerts: Conducting sample analysis to assess the effectiveness and accuracy of the screening alert processing.

Controls relating to internal standards:

- Regulatory monitoring: Continuously monitoring and staying updated on relevant regulatory developments and changes.
- Analysis of discrepancies: Conducting analysis to identify any discrepancies between internal systems and applicable regulatory provisions, such as country lists, required documents, and KYC validation levels.
- Deployment of normative changes: Implementing necessary changes to client files and internal systems to align with regulatory requirements.

Controls relating to governance

Level 1: Ongoing

- Certification and training: Ensuring that all individuals involved in AML/CFT procedures, including new personnel, certify their awareness of the procedures.
- Providing training, both internally and externally, to new employees and conducting annual training for "relevant persons" such as the compliance team and client onboarding staff.

Level 2: Annually

- Verification of training: Verifying the conduct of training sessions and maintaining attendance records to ensure compliance with AML/CFT training programs.

These controls and processes aim to ensure the effective implementation of AML/CFT measures, mitigate the risks of money laundering and terrorist financing, and comply with regulatory requirements.

7.2 Organisation of the AML/CFT KYC Team

The AML/CFT KYC (Know Your Customer) team is crucial for the effective implementation of AML/CFT measures. While the specific structure may vary depending on the company's size and operational requirements, the following elements are typically considered:

1.) Compliance Officer (CO): The CO is responsible for overseeing and managing the AML/CFT program within the organization. They ensure that the company adheres to relevant laws, regulations, and guidelines and implement effective AML/CFT controls.

2.) AML/CFT Team: This team consists of dedicated professionals responsible for conducting KYC procedures, monitoring transactions, investigating suspicious activities, and ensuring compliance with AML/CFT regulations. The team may include:

a. KYC Analysts: These individuals are responsible for gathering, verifying, and updating customer information, performing risk assessments, and maintaining client files in accordance with AML/CFT policies and procedures.

b. Transaction Monitoring Analysts: They monitor customer transactions on an ongoing basis, analyze patterns, and identify potentially suspicious activities or red flags.

c. Investigations Team: This team is responsible for conducting in-depth investigations into suspicious activities, analyzing transaction data, gathering additional information, and preparing reports for submission to the Financial Intelligence Unit (FIU).

d. Compliance Manager: This role involves overseeing the overall compliance function, ensuring adherence to AML/CFT regulations, and liaising with regulatory authorities.

3.) Internal Support Functions: Other departments within the organization may provide support to the AML/CFT team. These functions can include IT support for maintaining and upgrading AML/CFT systems, Legal and Compliance for legal advice and guidance, and Operations for coordination of customer onboarding and ongoing due diligence processes.

The organization of the AML/CFT KYC team should promote effective communication, collaboration, and information sharing among team members, enabling efficient monitoring and reporting of suspicious activities. The team should also stay updated on the latest AML/CFT regulations, undergo regular training, and participate in professional development activities to enhance their knowledge and skills in combating money laundering and terrorist financing

7.2.1 The Compliance Officer (CO)

The Compliance Officer (CO) is crucial in ensuring the effective implementation and oversight of the AML/CFT (Anti-Money Laundering/Counter Financing of Terrorism) program within the Company.

Here are the key responsibilities and qualifications of the CO based on the information provided:

1.) Qualifications and Appointment:

- The CO must possess at least five years of relevant experience in a compliance function, demonstrating their expertise in AML/CFT matters.
- The CO should be approved by the Dubai Virtual Assets Regulatory Authority (VARA) as a fit and proper person, ensuring their integrity and suitability for the role.
- The CO should be a resident in the UAE or hold a UAE passport.

- The CO must be a full-time employee of the Company, dedicated to fulfilling their AML/CFT responsibilities.
- The CO reports directly to the Board, indicating their senior position within the organization.

2.) Training and Policies:

- The CO is responsible for ensuring that the Board and staff members are properly trained and have a comprehensive understanding of AML/CFT laws and regulatory requirements, particularly those relevant to Virtual Asset (VA) activities.
- The CO develops and implements AML/CFT policies and procedures, which serve as the framework for the Company's compliance efforts.

3.) Risk Assessment and Compliance:

- The CO conducts AML/CFT risk assessments to identify and evaluate the risks faced by the Company.
- Based on the risk assessment findings, the CO implements necessary changes to the Company's policies and procedures to address the identified issues and risks effectively.

4.) Monitoring and Reporting:

- The CO monitors and reports suspicious transactions, ensuring that any red flags or suspicious activities are promptly identified and appropriately handled.
- If there is non-compliance with any Federal AML-CFT Laws, the CO takes the necessary corrective actions.
- On a quarterly basis, the CO reports to the Board on the effectiveness of the Company's AML/CFT policies and procedures, highlighting any policy failures or non-compliance with Federal AML-CFT Laws.
- The quarterly reports should also include a summary of all Anonymity-Enhanced Transactions and the clients involved during that period.

5.) Reporting to VARA:

- The CO makes the reports available to VARA upon request, ensuring transparency and compliance with regulatory requirements.

It is important to note that the specific responsibilities and requirements of the CO may vary depending on the jurisdiction and regulatory framework in which the Company operates.

7.2.2 The FIU Reporting Correspondent

The role of the FIU reporting correspondent within the Company is critical for ensuring effective communication and reporting of suspicious transaction reports to the Financial Intelligence Unit (FIU). Here are the key responsibilities and considerations for the FIU reporting correspondent based on the provided information:

1.) Designation and Independence:

- The Company must designate a FIU reporting correspondent who possesses the necessary independence and access to information required to carry out their responsibilities effectively.
- The reporting correspondent should hold a position within the Company that enables them to fulfill their duties independently and have access to relevant information.

2.) Functions of the Reporting Correspondent:

- The reporting correspondent is responsible for transmitting suspicious transaction reports to the FIU. This includes preparing and submitting the reports in accordance with the prescribed procedures and requirements.
- The reporting correspondent serves as the interface between the Company and the FIU. They receive acknowledgements of receipt of suspicious transaction reports from the FIU and handle requests for the communication of documents or additional information as requested by the FIU.

3.) Exceptional Reporting:

- In exceptional cases, any manager at the top management level may assume the role of the reporting correspondent and initiate the reporting to the FIU directly.
- This exceptional reporting may occur due to the urgency of the situation or specific circumstances. It is important that such reports are promptly confirmed by the authorized person within the Company.

4.) CO as the FIU Reporter:

- If no special person is designated as the reporting correspondent within the Company, the function of the FIU reporter is performed by the Compliance Officer (CO).
- In the absence of a designated reporting correspondent, the CO assumes the responsibility of reporting suspicious transactions to the FIU.

It is essential for SUNMONEY SOLAR GROUP to establish clear protocols and procedures for the designation of the reporting correspondent, ensuring their independence, access to information, and adherence to regulatory requirements for reporting suspicious transactions to the FIU.

7.2.3 The Responsible team for KYC

The KYC Team within the Company plays a crucial role in ensuring compliance with Know Your Customer (KYC) requirements. Here are the key responsibilities of the KYC Team based on the provided information:

1.) Data Collection and Compilation:

- The KYC Team is responsible for collecting and compiling all necessary data required for client identification and the onboarding process.
- This includes gathering relevant information such as client identification documents, proof of address, beneficial ownership details, and any other necessary documentation as per regulatory requirements.

2.) Client Identification:

- The KYC Team ensures that the client's identity is verified and that all required KYC information is obtained.
- They conduct due diligence checks on clients to establish their identity, assess their risk profile, and gather information necessary for ongoing monitoring.

3.) Alert Handling and Reporting:

- The KYC Team monitors client accounts and transactions on an ongoing basis.

- If any alerts or red flags indicating potential suspicious activity or non-compliance with AML/CFT regulations are identified, the KYC Team informs the CO.
- The CO, in turn, will further investigate and determine if the alert warrants reporting to the relevant authorities, such as the FIU.

It is important for the KYC Team to work closely with the CO to ensure that any alerts or suspicious activities are promptly communicated for appropriate investigation and potential reporting. This collaboration helps maintain a robust AML/CFT framework within the Company and facilitates effective risk mitigation and compliance with regulatory obligations.

8	Record Keeping

8.1 Record Keeping

The provided information highlights the recordkeeping requirements for the Company in accordance with the Federal AML-CFT Laws. Here's a summary:

1.) Crypto Assets Transaction Records:

- The Company is required to retain records of all crypto assets transactions, including operational and statistical records.
- These records encompass documents and information related to transactions executed or processed by the Company, regardless of whether they are recorded on public distributed ledgers.

2.) Customer Due Diligence (CDD) Records:

- The Company must maintain comprehensive CDD records, including documentation, information, and results from the investigation and analysis of clients' activities.
- This includes account files, business correspondence, and any relevant records pertaining to clients.

3.) Third-Party Engagement Records:

- The Company should keep records relating to third parties engaged to carry out CDD on its behalf.
- These records may include information about the third-party service providers and their activities in performing CDD procedures.

4.) Ongoing Monitoring Records:

- The Company is required to retain records related to the ongoing monitoring of business relationships with clients.
- This includes information and documentation gathered during the monitoring process to assess and mitigate risks associated with clients' activities.

5.) Suspicious Transaction Reports:

- The Company must keep records of suspicious transaction reports made in accordance with Rule III.F of the Compliance and Risk Management Rulebook.
- These records would include the details and supporting information related to the reported suspicious transactions.

Retention Period:

- The Company is mandated to retain all the aforementioned records for a minimum period of five (5) years.
- This duration ensures compliance with the recordkeeping requirements under the Federal AML-CFT Laws.

Confidentiality:

- The Company is responsible for ensuring the confidentiality of the information obtained during the fulfilment of AML/CFT requirements.
- Counterparty and transaction information should be kept confidential, safeguarding the privacy and security of such sensitive data.

SUNMONEY SOLAR GROUP, like any other company operating in the cryptocurrency space, to establish and maintain robust recordkeeping practices to demonstrate compliance with AML/CFT regulations.

SUNMONEY SOLAR GROUP can demonstrate its commitment to AML/CFT compliance, facilitate effective monitoring and oversight of its operations, and ensure regulatory authorities have access to necessary information when required. It is advisable for SUNMONEY SOLAR GROUP to consult with legal and compliance professionals to ensure they have implemented appropriate recordkeeping practices in line with relevant regulations and requirements.

9	**Responsibilities**

9.1 **Responsibilities**

The responsibilities outlined in your statement demonstrate the distribution of roles and obligations within the company's AML/CFT framework. Here's a summary of the key responsibilities for each department and employee:

The Board:

- Ensuring governance and oversight of the company's risk management framework and controls regarding money laundering (ML) and terrorist financing (FT).

Internal Audit (3rd level):

- Reviewing and auditing the entire company to assess adherence to processes and procedures based on the Board-approved audit plan.
- Providing support to monitor adherence to the AML/CFT Policy through its own mandate.

Compliance Department (2nd level):

- Managing overall compliance with laws and regulations, including conducting regular compliance reviews and making recommendations for improvements.
- Assisting in the decision-making process of escalating internal suspicious activity reports to the Financial Intelligence Unit (FIU).
- Advising on how to proceed with work to prevent tipping off and ensure effective investigations.

- Overseeing staff training on money laundering throughout the organization, regardless of office locations.
- Testing the operational effectiveness of key controls.

Risk Department (2nd level):

- Ensuring the establishment of risk frameworks, analyses, and underlying processes and procedures to appropriately manage ML/FT risks.
- Designing risk control frameworks and key controls.
- Conducting risk assessments to identify and assess the risk of ML/FT activities.

Business Departments:

- Ensuring the implementation of controls and systems to adhere to Compliance and Risk frameworks.
- Ensuring compliance with policies, procedures, and processes related to AML/CFT.
- Acting as risk owners within their respective departments.

Employees, Consultants, and Associated Persons:

- Complying with the company's AML/CFT Policy, standards, and controls.
- Familiarizing themselves with and adhering to relevant company processes and procedures for AML/CFT compliance.
- Reporting suspicions or red flags of ML/FT activities to the CO promptly.
- Completing all required company training programs.

It is important for each department and individual within the organization to understand their respective responsibilities and actively contribute to the company's efforts to combat money laundering and terrorist financing.

10	Anti-Bribery and Corruption

10.1 Anti-Bribery and Corruption

Company's commitment to conducting business with honesty, ethics, and a zero-tolerance approach towards bribery and corruption. Here are the key points regarding anti-bribery and corruption measures:

1.) Conducting Business Ethically:

- The Company is obligated to conduct all business dealings and relationships in an honest, fair, and professional manner.
- The Board and all staff members are expected to act with integrity in their business interactions.

2.) Prohibited Actions:

a. Bribery and Corruption Offenses:

- Giving, promising, or offering payments, gifts, or hospitality to a third party with the expectation of receiving a business advantage or to reward a business advantage already given.

b. Facilitation Payments:

- Giving, promising, or offering payments, gifts, or hospitality to a third party to expedite routine procedures.

c. Improper Acceptance of Payments or Gifts:

- Accepting payments, gifts, or hospitality from a third party if it's known or suspected that such offerings are made with the expectation of receiving a business advantage in return.

d. Threats or Retaliation:

- Prohibiting any threats or retaliation against Board members or staff who refuse to commit bribery offenses or raise concerns about such activities.

e. Breach of Anti-Bribery and Corruption Rules:

- Preventing engagement in any activity that may lead to a violation of the anti-bribery and corruption rules stated in the Compliance and Risk Management Rulebook.

3.) Monitoring and Addressing Deficiencies:

- The CO is responsible for regularly monitoring the effectiveness of anti-bribery and corruption measures.
- Any identified deficiencies should be addressed promptly and appropriately.

By maintaining strict adherence to these anti-bribery and corruption provisions, SUNMONEY SOLAR GROUP

aims to mitigate the risk of engaging in illicit activities and ensure a culture of integrity throughout its operations.

11	Training

11.1 Training

The training aspect of AML/CFT and anti-bribery and corruption is crucial to ensure that relevant personnel are knowledgeable about the requirements and measures adopted by the Company. Here are the key points related to training:

1. Training Scope:

- The training covers the local AML/CFT and anti-bribery and corruption requirements of the jurisdiction where the Company operates, as well as the specific measures implemented by the Company.
- The training ensures that employees understand their obligations and responsibilities regarding AML/CFT and anti-bribery and corruption.

2. Training Frequency:

- Training sessions are conducted on a regular basis, with a minimum frequency of at least once a year.
- The purpose is to keep personnel updated on any changes in regulations and reinforce their understanding of AML/CFT and anti-bribery and corruption measures.

3. Responsibility for Training:

- The CO is responsible for arranging the training sessions and ensuring their effective delivery.

- The CO coordinates and oversees the training program to ensure its compliance with regulatory requirements and internal policies.

4. Training for New Employees:

    - New employees are prioritized for training, and it should be provided as soon as possible after they join the Company.
    - This ensures that new hires are familiarized with the Company's AML/CFT and anti-bribery and corruption policies and procedures from the outset.

5. Documentation and Recordkeeping:
    - Attendance records for training sessions are systematically filed and archived in the HR departments.
    - Certificates given to employees as evidence of their completion of the training are also archived in the HR files.

By conducting regular training sessions and maintaining proper documentation, the Company aims to ensure that its employees are well-informed, compliant with regulations, and equipped to effectively address AML/CFT and anti-bribery and corruption risks in their roles.

12	Annual Review

12.1 Annual Review and Update

The annual review and update of the AML/CFT Policy, as well as the regulatory watch, are important aspects of maintaining an effective and up-to-date compliance framework. Here are the key points related to these processes:

1. Annual Review:

    - The CO is responsible for conducting an annual review of the AML/CFT Policy.
    - The purpose of the review is to ensure that the Policy remains current, accurate, and aligned with international best practices, evolving FATF Recommendations, and changing requirements.
    - Any necessary updates or revisions to the Policy are made during the annual review process.

2. Communication of Policy Changes:

    - When changes are made to the Policy, a new copy is made available to all personnel within the Company.
    - This ensures that employees have access to the most recent version of the Policy and are aware of any updates or modifications.

3. Documentation and Recordkeeping:

    - All versions of the Policy, including past revisions, are documented and retained for a period of five years.
    - This allows for reference and historical tracking of changes to the Policy over time.

4. Clarification and Inquiries:

    - If employees have any questions or need clarification regarding the Policy, they should refer to the CO.

- The CO serves as the point of contact for addressing inquiries related to the AML/CFT Policy.

12.2 Regulatory Watch:

- The CO is responsible for the regulatory watch, which involves staying informed about changes in laws, regulations, and recommendations related to AML/CFT.
- The CO undergoes dedicated training and subscribes to various legal and regulatory information feeds to stay updated.
- This includes subscribing to RSS feeds of local competent authorities, FATF, and the FIU, as well as regularly consulting updates, instructions, Q&A, and FATF recommendations provided by local competent authorities.

By conducting annual reviews, maintaining proper documentation, and staying informed through regulatory watch, the Company ensures that its AML/CFT Policy remains effective, compliant, and aligned with evolving standards and regulatory requirements.