HIKANOS

GROUP

HIKANOS ANTI-MONEY LAUNDERING POLICY

WWW.HIKANOS.COM

ANTI-MONEY LAUNDERING POLICY

This policy is to set out the basis of standards for compliance with the principles and obligations as per the Anti-money laundering and Counter Terrorism Financing legislative international and domestic requirements (hereinafter referred to as Regulations"). References in this Policy to money laundering should also be interpreted as references to terrorist financing.

OVERVIEW

Complying with the Regulations is an on-going obligation to maintain policies and procedures which are intended to combat money laundering. This Policy and the relevant internal procedures should be properly supported by management controls, kept up to date and communicated to staff. The Company should adopt a risk based approach, varying the measures taken in light of the assessed risk of money laundering.

Key to the prevention of money laundering is:

- monitoring
- multilevel identification of customers; including simplify due diligence with the only requirement to identify the CLIENT and no requirements to verify the information; standard Due Diligence ; Enhance Due Diligence (required where the client and product/service combination is considered to be a greater risk.)
- identification and reporting of knowledge or suspicions of money laundering;
- record keeping.

SUPPORTING POLICIES AND CONTROLS

Internal Policies and Procedures

The Company should maintain internal policies and procedures for:

- know your customer (KYC) and due diligence;
- reporting;
- record keeping;
- internal management controls;
- risk assessment and management;
- the monitoring and management of compliance; and
- the internal communication of such policies and procedures.

The Company's policies and procedures should take a risk based approach. The Company's policies and procedures must:

- ensure that complex or unusually large transactions, or unusual patterns of transactions, are identified and scrutinized;
- specify the additional measures that will be taken to prevent the use of products and transactions which favour anonymity

The senior managers of the Company are responsible for ensuring that the Company’s policies and

procedures are put in place and applied effectively so as to ensure proper assessment and management of the money laundering risks to the company.

Nominated Officer

The Company's policies and procedures must also nominate an individual to:

- receive disclosures of suspicious activity from the Company's staff; and report suspicious activity to the relevant authorities;
- ensure that staff disclose suspicious activity to the Nominated Officer;
- ensure that the Nominated Officer considers such disclosures and, if such there reasonable grounds for knowledge or suspicion of money laundering, reports suspicious activity to the relevant authorities.
- ensure that none of the reported to the relevant authority suspicious transactions is executed without prior approval of the competent authority.

'Knowledge' means knowledge of money laundering activity based on information which came to a member of staff or the Nominated Officer in the course of the business of the Company.

'Suspicion' means an opinion based on information or circumstances but without any certainty or proof.

Controls and Communications

The Company must ensure that internal management controls are put into place in order to be aware of potential money laundering.

Internal controls should include:

- identification of senior management responsibilities;
- regular provision of information to senior management on the risks of money laundering;
- relevant staff training on policies and procedures;
- documentation of the risk management policies and procedures;

The Company should regularly assess its policies, procedures and management controls to ensure the risks of money laundering continue to be known and managed.

RISK BASED APPROACH

A risk based approach is an approach which is a cost effective and proportionate way to manage the risk of money laundering. In implementing a risk based approach, the Company should consider: the risk posed by the customer.

The following customers and behavior should be considered riskier:

- If the customer is from a country from FATF, EU lists, OFAC list or entered in some of those lists:

  1. European Union Consolidated List 2. European Union Terrorist List 3. Financial Action Task Force Non-Cooperative Countries and Terrorists 4. Her Majesty's Treasury – also known as Bank

of England (Consolidated List) 5. Her Majesty's Treasury (Investment Ban List) 6. Interpol List of Most Wanted – Recent Event Red Alerts 7. US Treasury Office of Foreign Assets Control (OFAC) Specially Designated Nationals 8. US Treasury Office of Foreign Assets Control (OFAC) Sanctioned Countries 9. US Department of State Foreign Terrorist Exclusion List 10. United Nations Sanction List.

- If the customer's response is unclear or even there is no response.
- If the customer's behavior is unusual
- If the customer illogically changes the transaction model he/she used
- If the customer is not reluctant to provide information about the source of the funds for a deposit
- If the customer attempts to circumvent the requirement to provide the necessary sufficient personal information when registering to use the Company's products and services.
- If the customer wants to withdraw funds without concerning the fees much
- If the customer wants to give bribe, in order to speed up the the withdrawal process.
- If the customer deposits much more money than he/she is expected to have (as per his/her profile)
- If the amount of the deposited funds do not correspond to his/her profile history.
- If the customer attempts to make a fund transfer to another customer if there is no coherent economic rationale for the transaction
- If the customer is not reluctant to identify him/herself, including upon request
- If the customer demands details about the Company's internal AML/CTF procedures and limits.
- If the customer withdraws his funds in very short terms (within 24 hours) after depositing and without purchasing any product or service
- If the customer speaks about crimes or property obtained by such an act.
- If the customer submits falsified ID or other documents in order to use the Company's products and services;

- If a new customer makes a large one-off transaction;
- If the customer holds a public or governmental position;
- If the customer is operating in jurisdictions known to have a high risk of money laundering.
- If the risk posed by the client's behaviour is sufficient.
- If the customer appears to act on behalf of another person;
- If the client shows willingness to bear uncommercial penalties or other risks.

The Company should monitor the risk of money laundering by being aware of patterns of business transactions, including:

- unusual increase of the business of an existing customer;
- transactions which are not relevant to the customer's known activity;
- unusual increase of the activity at particular points of time; and
- unfamiliar or untypical types of customers or transactions.

Risk based control procedures include:

- customer identification;
- verifying customer identification; and
- additional customer identification or implementing enhanced customer due diligence in the case of higher risk.

CUSTOMER DUE DILIGENCE, IDENTIFICATION, MONITORING AND RESTRICTIONS

Customer Due Diligence

The object of customer due diligence is to identify customers and verify their identity.

Customer due diligence should include checking the list of financial sanctions targets listed on the competent authorities website. The Company should not do business with a person or entity subject of a financial sanctions.

The Company should be able to demonstrate that its due diligence (KYC) measures are appropriate in light of the Company's risk of money laundering by. Steps in the Know Your Customer (KYC) process are:

- identification of customers; including simplify due diligence with the only requirement to identify the CLIENT and no requirements to verify the information (appropriate where it is hardly possible or there is a low risk of Company's services or customer becoming involved in money laundering or terrorist financing).

The business relationship should be continually monitored for trigger events which may create a requirement for further due diligence in the future.

- These are generally situations where there is a potential risk but it is unlikely that these risks will crystallize (a risk that happened and loss occurred.

The standard due diligence procedure requires customers' identification as well as verifying of the customer's identity . In addition, the Company ensures gathering of information so as to understand the nature of the business relationship with the customer. This due diligence procedure should give us confidence that we know who our customers are and that our services or products are s not being used for money laundering or for any other criminal activity.

As with simplified due diligence we monitor our customers throughout all the business relationship, which enables us highlighting any potential trigger events that may result in further due diligence being required.

- Enhance Due Diligence is required where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high risk situation generally occurs where there is an increased opportunity of money laundering or terrorist financing through the service and product provided to the customer.

What the enhanced due diligence actually entails will dependent on the nature and severity of the risk. The Company's additional due diligence could take many forms - from gathering additional information to verifying the customers identity or source of income or perhaps an adverse media check. The checks should be relative and proportionate to the level of risk identified and should give confidence that any risk has been mitigated and that the risk is unlikely to crystallize

The Company asks its customers to state whether or not they hold or have previously held a prominent public government function and ensure that such customers are treated as high risk.

Identification and Verification

Identification can be documentary, electronic or a combination of both. A record should be kept of all evidence taken to establish the customer's identity. Documentation of identity should be supplemented with additional identification such as a recent utility bill or a bank statement which is less than 3 months' old and which shows the customer's name and address.

Ongoing Monitoring

The Company should monitor customer activity on an ongoing basis.

Ongoing monitoring includes:

- scrutinising transactions, including the source of funds, the directions of funds; changes of transactions models,
- ensuring information about customers is kept up to date

Monitoring may take place as part of a review of previous transactions and can be manual or automated. Staff should be trained in conducting ongoing monitoring.

RECORD KEEPING

Sufficient records should be kept to demonstrate compliance with the Regulations, including records of:

- policies and procedures;
- controls and communication;
- customer and transaction risk analysis;
- customer due diligence, including evidence of customer identity and any supporting documentation;
- ongoing monitoring; and
- transactions and business records, in a form sufficient to compile an audit trail.

Records should be kept during the business relationship and further for 5 years as from , the date the relationship with the customer ends.

Under no circumstances the COMPANY, its employees, consultants, or representatives will engage in negotiation with terrorists. Suspicious behavior or actions will be immediately reported to competent authorities.

The COMPANY, under the protection of the safe harbor from liability, may voluntarily receive or otherwise share information with any of the other financial or governmental institution regarding individuals, entities or other organizations for purposes of identifying and where appropriate reporting activities that may involve possible terrorist or money laundering activities.

Anti-Money Laundering (AML) Withdrawals Restrictions

In order to comply with generally acceptable rules and regulations, CLIENTs can only withdraw funds to their own accounts (bank account, bank card, Bitcoin, Perfect money account,etc.). The Company will execute withdrawal requests only of CLIENTs with approved KYC documents. Withdrawal requests to

third parties are not allowed. In case of an attempt to execute transactions, suspected by the Company to be related to money laundering or any other criminal activity, the Company reserves the rights to suspend such operations and has complete discretion to temporary block or terminate the relationship with the suspected existing CLIENTs and to act according to the internal reporting procedure.

All employees and agents have been provided with a copy of the present policy. All new employees and agents will be provided with a copy of this policy at the time of their hiring.

We appreciate your understanding and full cooperation in relation to the implementation of this policy.

All inquiries regarding this policy shall be directed to the Legal and Compliance Department