

## **AML Policy**

### **Zenith Origin Holding Ltd**

This Policy is in accordance with the general principles, laws, regulations and directives for combating money laundering. The Company is taking security measures and has adopted policies, practices and procedures that promote high ethical and professional standards and prevent the Company from being used, intentionally or unintentionally, by criminal elements.

The Company has put in place Know Your Customer (KYC) procedures as an essential element for service, risk management and control procedures. Such procedures include:

- Risk-based customer acceptance policy
- Customer identification and verification
- On-going monitoring of high-risk accounts and transactions
- Risk management

The Company is obliged not only to establish and verify the identity of its customers, but also to monitor on an ongoing basis the account activity to detect those transactions that do not conform with the normal or expected transactions for that customer or type of account. KYC constitutes a core feature of services' risk management and control procedures. The intensity of KYC procedures beyond these essential elements is tailored to the degree of risk.

#### **1. CUSTOMER ACCEPTANCE POLICY**

The Company maintains clear customer acceptance policies and procedures, including a description of the types of customer that are likely to pose a higher than average risk. Before accepting a potential client, KYC and due diligence procedures are followed, by examining the following factors:

- customers' background
- country of origin
- Public or high-profile position (i.e. PEPs)
- Client's age (Above 18 years-old)
- linked accounts
- Business activities
- Any other risk indicators.

Enhanced due diligence is essential for an individual from high-risk countries, Politically exposed persons, complex structures and high net worth clients but whose source of funds is unclear. New clients' money is transferred through a reputable bank. Banks have their own anti-money laundering procedures. A decision to enter into business relationships with higher risk customers, such as politically exposed persons, is taken exclusively at senior management level. Company's operations procedures in terms of accepting new traders and compliance requirements, accepting funds and withdrawal procedures:

- Back office oversees the documents provided in order to identify and verify the client;
- The depositing method must be examined so that there will be no suspicious activity and in order to comply with the Anti Money Laundering protocols.

## **2. CUSTOMER IDENTIFICATION**

Customer identification is an essential element of KYC standards. For the purposes of this paper, a customer includes:

- The person or entity that maintains an account with the company or those on whose behalf an account is maintained (i.e. beneficial owners);
- The beneficiaries of transactions conducted by professional intermediaries;
- Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the company.

The Company maintains a systematic procedure for identifying and verifying of new customers and cannot enter into a service relationship until the identity of a new customer is satisfactorily verified.

Procedures document and enforce policies for identification of customers and those acting on their behalf. The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit. The Company pays special attention in the case of non-resident customers and in no case are short-circuit identity procedures followed just because the new customer is unable to present enough documents and information to satisfy the KYC and due diligence procedures.

The customer identification process applies naturally at the outset of the relationship. To ensure that records remain up-to-date and relevant, the Company undertakes regular reviews of existing records. An appropriate time to do so is when a transaction of significance takes place, when customer documentation standards change substantially, or when there is a material change in the way that the account is operated.

However, if the AML/CFT (anti-money laundering and countering the financing of terrorism) Supervisor for the Company (AML/CFT Supervisor) becomes aware at any time, through compliance and/or AML/CFT Supervisor reviews, that it lacks sufficient information about an existing customer, immediate steps are taken to ensure that all relevant information is obtained as quickly as possible. The Company can be exposed to reputational risk, and should therefore apply enhanced due diligence to such operations.

Private accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalized investment company. In each case reputational risk may arise if the company does not diligently follow established KYC procedures. All new clients and new accounts are approved by at least one person the Companies Customer Financial Officer or its own AML/CFT Officer. In case of a new high-risk customer, the final decision is taken by the Companies managing director. Particular safeguards have been put in place internally to protect confidentiality of customers and their business. The

Company ensures that equivalent scrutiny and monitoring of these customers and their business is conducted, e.g. it is available to be reviewed by the AML/CFT Supervisor and auditors.

The Company maintains clear standards and policies, on what records must be kept for customer identification and individual transactions. Such practice is essential to permit the Company to monitor its relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

As the starting point and follow-up of the identification process, the Company obtains customer identification papers and retain copies of them for at least seven years after an account is closed. The Company also retains all financial transaction records for at least seven years from the date when the Company's relationship with the client was terminated or a transaction was completed.

