



## **AML and KYC Policy**

It is the policy of Blue Sun Capital Ltd and its affiliates, (hereinafter “the Company”) to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company requires its officers, employees and affiliates to adhere to these standards in preventing the use of its products and services for money laundering purposes.

The Company shall apply at least the following due diligence measures to ALL the customers:

- Identification of a customer and verification of the submitted information
- Identification and verification of the customer’s representative, if applicable
- Identification and verification of the beneficial owner, if applicable
- Verifying if the customer is a politically exposed person (a.k.a. PEP) status
- Screening the customer against international sanctions

For the purposes of the Policy, money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

Generally, money laundering occurs in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler’s checks, or deposited into accounts at financial institutions. At the “layering” stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Each employee of the Company, whose duties are associated with the provision of products and services of the Company and who directly or indirectly deals with the clientele of the Company, is expected to know the requirements of the applicable laws and regulations which affect his or her job responsibilities, and it shall be the affirmative duty of such employee to carry out these responsibilities at all times in a manner that complies with the requirements of the relevant laws and regulations.

The laws and regulations include, but not limited to: “Customer Due Diligence for Banks” (2001) and “General Guide to Account Opening and Customer Identification” (2003) of Basel Committee of banking Supervision, Forty + nine Recommendations for Money Laundering of FATF, USA Patriot Act (2001), Prevention and Suppression of Money Laundering Activities Law (1996).

To ensure that this general policy is carried out, management of the Company has established and maintains an ongoing program for the purpose of assuring compliance with the relevant laws and regulations and the prevention of money laundering. This program seeks to coordinate the specific regulatory requirements throughout the group within a consolidated framework in order to effectively manage the group's risk of exposure to money laundering and terrorist financing across all business units, functions, and legal entities.

Each of the affiliates of the Company is required to comply with AML and KYC policies.

All identification documentation and services records shall be kept for the minimum period of time required by local law.

All new employees shall receive anti-money laundering training as part of the mandatory new-hire training program. All applicable employees are also required to complete AML and KYC training annually. Participation in additional targeted training programs is required for all employees with day to day AML and KYC responsibilities.

## KYC policy

Each user has to provide the required documents according to the chosen deposit method in 14 days from the date of the first deposit.

- If credit/debit card is used to deposit funds you have to provide a Proof of Identification (POI), Proof of Address (POA) and a copy of the Credit/Debit card that you used for payment.
- If bank transfer is used to deposit funds, you must provide a Proof of Identification (POI) and a Proof of Address (POA).

The verification process can take a week, and users will be notified once the account is verified. Verification status can also be followed in the client zone.

In the event that the documents are rejected, an email with a clear explanation of what is needed to provide will be sent.

In order for the above-mentioned documents to be accepted they have to meet the following criteria:

- Documents have to be in one of the following formats: .PDF, .PNG or .JPEG
- Documents can not be cropped, cut or blurry.
- Documents have to be colored and all corners have to be visible.

- All information on the documents has to be legible.
- No information can be covered or altered.

#### Proof of Identity (POI)

A passport is the preferred proof of identity, alternatively, an ID card can be used for the verification process. If the document is double-sided the back side has to be provided as well.

The document should contain the user's following information:

- full name
- date of birth
- a clear photograph
- issue date
- expiry date (if applicable)

#### Proof of Address (POA)

POA document should contain users:

- full name
- address
- issue date, which should be no older than 3 months
- name and/or logo of the issuer

Proof of Address can be one of the following:

- Bank Statement
- Credit Card Statement
- Electricity, Water or Gas Bill
- Internet Bill
- Landline Phone Bill
- Tax letter or Bill
- House Rental Official Agreement – Issued by Government
- Letter from your local municipality