



## **AML/KYC Policy**

For purposes of this Policy, “us,” “we,” or “our” refer to Astol Advanced Limited (19H Maxgrand Plaza No.3 Tai Yau Street San Po Kong, Kowloon Hong Kong, reg.num 3152800) d/b/a ASTL Token.

Our Anti-Money Laundering and Know Your Customer Policy (hereinafter - the “AML/KYC Policy”) are designated to prevent and mitigate possible risks of us being involved in any kind of illegal activity.

https://astl.io Services are not offered for use to persons or legal entities located in or have their habitual residence or registered office in the United States of America or any other country where https://astl.io does not offer Services. For as long as you maintain your registered account at https://astl.io, you represent and warrant that you are not located in or a resident of the United States of America. You are also not allowed to use the Services if you are located in or are a resident of a Prohibited Jurisdiction. “Prohibited Jurisdiction” means any state, country, territory or other jurisdiction (1) that at any given time is subject to broad-based, geographically oriented sanctions by the United Nations, The Central Bank of Ireland, the European Union, OFAC, or is identified as a “call to action” jurisdiction on the FATF's list of “High-Risk and Other Monitored Jurisdictions”; (2) where your use of the Services would be illegal or otherwise violate any applicable law, or (3) that https://astl.io determines in its sole discretion is ineligible for access to and use of the Services.

Both international and local regulations require us to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity of our customers.

AML/KYC Policy covers the following matters:

- Compliance Officer;
- Risk Assessment;
- Verification procedures;
- Monitoring Transactions.

### **Compliance Officer**

The Compliance Officer is the person, duly authorized by us, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of our anti-money laundering and counter-terrorist financing, including but not limited to:

- Collecting customers' identification information;
- Establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations;



- Monitoring transactions and investigating any significant deviations from normal activity;
- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;
- Updating risk assessment regularly;
- Providing law enforcement with information as required under the applicable laws and regulations.

The Compliance Officer is entitled to interact with law enforcement, which are involved in the prevention of money laundering, terrorist financing and other illegal activities.

### **Risk Assessment**

We, in line with the international requirements, have adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, we are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the identified risks. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

### **Verification procedures**

One of the international standards for preventing illegal activity is customer due diligence (“CDD”). According to CDD, we establish our own verification procedures within the standards of Anti-Money Laundering and “Know Your Customer” frameworks.

#### **a) Identity verification**

Our identity verification procedure requires the customer to provide us with reliable, independent source documents, data or information (e.g., national ID, international passport, bank statement, proof of address). For such purposes, we reserve the right to collect customer's identification information for the AML/KYC Policy purposes.

We will take steps to confirm the authenticity of documents and information provided by the customers. All legal methods for double-checking identification information will be used and we reserve the right to investigate certain customers who have been determined to be risky or suspicious.

We reserve the right to verify a customer's identity in an on-going basis, especially when their identification information has been changed or their activity seemed to be suspicious (unusual for the particular customer). In addition, we reserve the right to request up-to-date documents from the customers, even though they have passed identity verification in the past.

Customer's identification information will be collected, stored, shared and protected strictly in accordance with our Privacy Policy and related regulations.



Once the customer's identity has been verified, we are able to remove ourselves from potential legal liability in a situation where our services are used to conduct illegal activity.

#### **b) Card verification**

The customers who use payment cards connected with our services can be asked to pass card verification. It may include:

- Scan/photo of the card statement of the page which shows there was a payment for our services.
- Scans/photo of the payment card (both sides). We require cardholder name and signature, first 6 and last 4 digits of the card's number have to be clearly seen. CVV code and remain part of the card's number must be hidden by a piece of paper.
- Selfie, where the customer is holding clearly visible payment card in the hand (only first 6 and last 4 digits of the number have to be seen well) plus a piece of paper with a sign "astl.io" and current date for the moment customer is taking the selfie.
- Any other documents confirming that the payment has been authorized by the cardholder indeed.

#### **Monitoring Transactions**

The customers are known not only by verifying their identity (who they are) but, more important, by analyzing their transactional patterns (what they do). Therefore, we rely on data analysis as a risk-assessment and suspicion detection tool. We perform a variety of compliance-related tasks, including capturing data, filtering, recordkeeping, investigation management, and reporting. System functionalities include:

a) A daily check of customers against recognized "black lists" (e.g. OFAC), aggregating transfers by multiple data points, placing customers on watch and service denial lists, opening cases for investigation if it is essential, sending internal communications and filling out statutory reports, if applicable;

b) Case and document management.

With regard to the AML/KYC Policy, we will monitor all transactions and it reserves the right to:

- ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
- request the customer to provide any additional information and documents in case of suspicious transactions;
- suspend or terminate customer's account when we have reasonable suspicion that such customer is engaged in illegal activity.

The above list is not exhaustive and the Compliance Officer will monitor customers' transactions on a day-to-day basis.