The Company appreciates your trust and is committed to protect its Users. Below, there is Anti Money Laundering & “Know Your Client” policy (hereinafter – “Policy”), the terms used herein are similar to those that were used in Privacy Policy (https://DYN.io/en/privacy-policy) and / or in Pre-order Agreement (https://DYN.io/en/pre-order-agreement).

Illicit financial flows can damage the integrity, stability and reputation of the Company. The purpose of this Policy is to prevent the Company from being used, intentionally or unintentionally, by criminal elements for money laundering activities or terrorist financing activities. KYC and AML procedures shall also enable the Company to know and understand its Users and its financial dealings better which, in turn, will help it to manage the risks prudently. Thus, this Policy has been framed by the Company for the following purposes:

• To prevent criminal elements from using Company or its Product for money laundering activities;

• To enable Company to know and understand its Users and their financial dealings better which, in turn, would help the Company to manage risks prudently;

• To put in place appropriate controls for detection and reporting of suspicious activities in accordance with applicable laws/procedures laid down;

• To comply with applicable laws and regulatory guidelines.

THIS POLICY COVERS THE FOLLOWING MATTERS:

1. IDENTITY VERIFICATION

1.1. It is Company’s own verification procedure, created in compliance with international standards and requirements:

• Company’s identity verification procedure requires the User to provide Company or its contractor with reliable, independent source documents, data or information (e.g., national ID, international passport, bank statement, utility bill). For this purposes Company reserves the right to collect User’s identification information for this Policy purposes.

• To confirm the authenticity of documents and information provided by Users, the Company shall take all the necessary steps. All legal and accessible methods for double-checking identification information shall be used.

• Company reserves the right to verify User’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 User).

• User’s identification information will be collected, stored, shared and protected strictly in accordance with the Company’s Privacy Policy (https://DYN.io/en/privacy-policy) and related regulations.

• Once the User’s identity has been verified, Company may remove itself from potential legal liability associated with subsequent actions of Users.

2. COMPLIANCE OFFICER

2.1. The Compliance Officer is the person, duly authorized by Company, whose duty is to ensure the effective implementation and enforcement of this Policy. It is the Compliance Officer’s responsibility

to supervise all aspects of Company's anti-money laundering and counter-terrorist financing, including but not limited to:

• Collecting Users' 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.

• 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.

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

2.3. The Company has the right to hire independent, duly authorized contractors for the purpose of compliance with this Policy.

3. RISK ASSESSMENT

3.1. Company, in line with the international requirements, has adopted a risk-based approach to combat money laundering and terrorist financing in all potential manifestations. By adopting a risk-based approach, Company is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the identified risks. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

3.2. As regards the risk assessment referred to above, Company shall:

• use it to improve its AML/KYC regime, in particular by identifying any areas where obliged subjects are to apply enhanced measures and, where appropriate, specifying the measures to be taken;

• identify, where appropriate, sectors or areas of lower or greater risk of money laundering and terrorist financing;

• use it to assist it in the allocation and prioritization of resources to combat money laundering and terrorist financing;

• make appropriate information available promptly to obliged subjects to facilitate the carrying out of their own money laundering and terrorist financing risk assessments.

3.3. As part of the User risk assessment, the following will act as Money Laundering Warning Signs based on guidance provided by Financial Action Task Force (FATF) – an international body set up to combat money laundering:

• User tells that the funds are coming from one source but then at the last minute the source changes;

• Evasiveness or reluctance to provide information;

• Incomplete or inconsistent information;

• Unusual Ethereum transfer or transactions;

• When Ethereum is coming from the list of “high -risk and non-co-operative jurisdictions” according to FATF;

• Negative public information available about the User.

3.4. In order to comply with international regulations and in order to balance the risk of driving transactions underground as a result of overly strict identification requirements against the potential terrorist threat posed by small transfers of funds, we shall imply the obligation to check whether information on the payer or the payee is accurate should, in the case of transfers of funds where verification has not yet taken place, be imposed only in respect of individual transfers of funds that exceed EUR 1 000, unless the transfer appears to be linked to other transfers of funds which together would exceed EUR 1 000 (in ETH equivalent).

4. USER’S OBLIGATIONS AND GUARANTEES

4.1. The User is obliged under this Policy:

• to respect and obey any requirements of the law, including internal policies, directed on fight against illegal activities, financial frauds, laundering and legalization of the money received in the illegal way;

• to exclude direct or indirect complicity of illegal financial activities and to any other illegal operations with use of the Company’s website;

• not to use Product or Token for any illegal or fraudulent action, or for any illegal or fraudulent Operations (including money laundering) according to the Applicable law;

4.2. User guarantees a legal origin, legal ownership and availability of the actual right to use the Ethereum transferred by User.

5. INVESTIGATION

5.1. Company reserves the right to investigate certain Users who have been determined to be risky, suspicious or resident in geographical areas of higher risk.

5.2. In case of suspicious or fraudulent funds replenishments, including any returns or cancellations of pre-orders or provision of incomplete or incorrect information, Company also reserves the right to cancel pre-order and to block User’s account, to cancel results of any financial operations performed by User and to investigate operations of doubtful nature owing to what to suspend such operations before clarification of the nature of emergence of Ethereum and the end of investigation.

6. LIABILITY

6.1. Refusal by Company of carrying out suspicious operations is not the basis for any Company’s responsibility before User and / or other third parties for non-execution of any liabilities in relation to User.

6.2. Company solely may terminate User’s account or refuse relevant pre-orders or applications if Company or its contractors will discover non-compliance with this Policy or other internal rules.

6.3. To ensure that the information that the Company holds on its customers is always accurate and up to date, Company shall, upon its sole discretion, determine the periodicity at which each User shall be, upon request, obliged to provide their KYC information anew to continue using Company Product.