ZOOM AML AND KYC POLICY

This Anti-Money Laundering and Know-Your-Customer Policy ("**this Policy**" or "**AML & KYC**") constitutes an agreement between **Zoom** ("**Company**" or "**us**" or "**we**" or "**our**") and you or the entity you represent ("**you**" or "**User**"). Please read this document carefully to be sure that you understand it. By viewing, accessing or using the Company website or by registering to take part in the token sale and the activities of the Company, you agree to this Policy as a binding legal agreement between you and us, without limitation or qualification. This Policy is designated to prevent and mitigate possible risks of Zoom being involved in any kind of illegal activity.

Both international and local regulations require Zoom 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 from its Users.

This AML & KYC Policy is a part of and incorporated within, and is to be read along with, our Terms of Use (the "**Terms**") and our Privacy Policy. Unless otherwise specified, or required by reasonable or necessary implication, terms in this AML & KYC Policy have the same meaning as terms defined and used elsewhere in our Terms of Use. To avoid doubt, all provisions within our Terms of Use, including but not limited to, the Subscription Agreement, apply equally and uniformly to this AML & KYC Policy.

We have the right, at any time, to change or modify the terms and conditions applicable to your use of our Services, or any part thereof (including this AML & KYC Policy), or to impose new conditions, including, but not limited to, adding fees and charges for use. Such changes, additions or deletions shall be effective immediately upon notice thereof. This notice may be given by means including, but not limited to, updating the "Last Updated" or "Last Changed" fields at the top of this document with the date of the current revision.

Any use of our Services by you after such notice shall be deemed to constitute acceptance by you of such changes, modifications or additions. Any amended Terms will apply prospectively to use of the Services after such changes become effective. It is important therefore that you review our Terms of Use and Privacy Policy on a regular basis to ensure that you are familiar with the terms in force from time to time and/or any changes made to them. If you do not agree to any amendments, you must discontinue using our Services and contact us to terminate your account.

You may either at the time of registering as a User; upon execution of any transactions; or periodically for purposes of updating records and on-going due-diligence (as specified under the various AML laws and international standards, or upon being directed by appropriate enforcement authorities), be required to take part in the User identification and verification process.

1. **Required Customer Information**
   We may collect the following information for the purposes of verification of identification:

   1.1. Natural persons:
   Name; date of birth; email address; phone number and residential address; photograph; copies or certified copy of any Valid Documents; documents pertaining to business/ financial status of such User (if prescribed by the Company);

   1.2. Legal persons:
   Business name; name, contact-details, photograph, and copy of Valid Documents of the authorized representative, one certified copy each of the certificate of incorporation/ registration Certificate (as the case may be); memorandum and articles of association/ partnership deed (as the case may be); board resolution/other authorization documents giving authority to the representative chosen to execute transactions on the Website;

   You must promptly update us of any changes to the customer information provided to us within three days of effecting such changes. You must file a fresh proof of address within three (3)

months of effecting any changes to the address mentioned as per the 'proof of address' submitted by you.

2. Verification procedures

One of the international standards for preventing illegal activity is customer due diligence ("CDD"). According to CDD, Zoom establishes its own verification procedures within the standards of anti-money laundering and Know-Your-Customer frameworks. Zoom may use third party services and software to identify and authenticate its customers.

2.1. Identity verification

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

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

Zoom 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). In addition, Zoom reserves the right to request up-to-date documents from the Users, even though they have passed identity verification in the past.

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

Once the User's identity has been verified, Zoom is able to remove itself from potential legal liability in a situation where its services are used to conduct illegal activity.

2.2. Card verification

The Users who are intended to use payment cards in connection with the Zoom's Services have to pass card verification in accordance with instructions available on the Zoom's Site.

3. Compliance Officer

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

a. Collecting Users' identification information.
b. 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.
c. Monitoring transactions and investigating any significant deviations from normal activity.
d. Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs.
e. Updating risk assessment regularly.
f. 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 prevention of money laundering, terrorist financing and other illegal activity.

4. Monitoring Transactions

The Users are known not only by verifying their identity (who they are) but, more importantly, by analyzing their transactional patterns (what they do). Therefore, Zoom relies on data analysis as a risk-assessment and suspicion detection tool. Zoom performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting. System functionalities include:

4.1. Daily check of Users against recognized "black lists" (e.g. OFAC), aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;

4.2. Case and document management.

With regard to the this Policy, Zoom will monitor all transactions and it reserves the right to:

4.3. ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer;
4.4. request the User to provide any additional information and documents in case of suspicious transactions;
4.5. suspend or terminate User's Account when Zoom has reasonable suspicion that such User engaged in illegal activity.
4.6. The above list is not exhaustive and the Compliance Officer will monitor Users' transactions on a day-to-day basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide.

5. Risk Assessment

Zoom, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, Zoom is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to 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.

We will undertake a risk assessment based on (a) sufficiency and adequacy of identification documents submitted by you; (b) your social and/or financial status; (c) nature and other similar information about your business/vocational activities; or (d) guidance notes circulated by various governmental and intergovernmental organizations. We may internally categorize you as a low-risk, medium-risk, or a high-risk User on the basis of the aforementioned assessment.

We will keep your risk categorization and related data confidential at all times, subject to any requests received from a competent law enforcement authority. In order to maintain the integrity of the risk assessment process, the results of your risk assessment and/or categorization will not be disclosed to you either.