ANTI-MONEY LAUNDERING POLICY

Braandsio Internet Private Limited

INTRODUCTION

This Anti-Money Laundering Policy ("**Policy**") prepared by **Braandsio Internet Private Limited**, a company incorporated under the laws of Republic of India under registered number U72900HR2022PTC107422, having legal and business address at: 792, LGF, New Rajinder Nagar, New Delhi - 110060 (the "**Company**"), website http://braands.io/

This Policy is prepared in accordance with **The Prevention Of Money-Laundering Act, 2002 (PMLA)** with all relevant amendments adopted and came into force on the 1st July 2005 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives with all relevant amendments adopted.

The Company created this Policy to decrease the risk of money laundering and terrorist financing associated with its business and the sale of its products.

This Policy emphasizes our individual obligation for adhering to anti-money laundering (also referred as "AML") and counter-terrorist financing (also referred as "CFT") legislation (and also with laws around the world, such as European Union Directives etc).

This Policy shall be disseminated to all Company personnel who manage, monitor, or oversee in any manner the Customers' transactions and are responsible for the implementation of the practices, measures, procedures, and controls established herein. Any employee who breaches the provisions in this Policy, or who allows others to break this Policy, may face appropriate disciplinary action, up to and including dismissal, as well as civil or criminal fines.

By no means this document shall not be read as an entire set of all policies, procedures and controls in place implemented by the Company for prevention of money laundering, financing of terrorism and other forms of illicit activity.

The Company shall regularly check whether the Policy is up-to-date and make necessary changes upon amendments to the regulations in force.

1. CUSTOMER DUE DILIGENCE AND CUSTOMER ACCEPTANCE PROCESS

2.

1.1. Customer due diligence ("**CDD**") is one of the main tools for ensuring the implementation of legislation aimed at preventing money laundering and terrorist financing and at applying sound business practices. CDD comprises a set of activities and practices arising from the organizational and functional structure of the Company and described in internal procedures, which have been approved by the directing bodies of the Company and the implementation of which is subject to control systems established and applied by internal control rules.

1.2. The purpose of CDD is to prevent the use of assets and property obtained in a criminal manner in the economic activities of credit institutions and financial institutions and in the services provided by them whose goal is to prevent the exploitation of the financial system and economic space of the Republic of India for money laundering and terrorist financing. CDD is aimed, first and foremost, at applying the **Know Your Client** ("KYC") principle, under which a Customer shall be identified and the appropriateness of transactions shall be assessed based on the Customer's principal business and prior pattern of payments. In addition, CDD serves to identify unusual circumstances in the operations of a Customer or circumstances whereby an employee of the Company has reason to suspect money laundering or terrorist financing.

1.3. CDD ensures the application of adequate risk management measures in order to ensure constant monitoring of Customers and their transactions and the gathering and analysis of relevant information. Upon applying the CDD measures, the Company will follow the principles compatible with its business strategy and, based on prior risk analysis and depending on the nature of the Customer's business relationships, apply CDD to a different extent.

1.4. CDD is applied based on a risk sensitive basis, i.e. the nature of the business relationship or transaction and the risks arising there from shall be taken into account upon selection and application of the measures. Risk-based CDD calls for the prior weighing of the specific business relationships or transaction risks and, as a result thereof, qualification of the business relationship in order to decide on the nature of the measure to be taken.

1.5. CDD measures are appropriate and with suitable scope if they make it possible to identify transactions aimed at money laundering and terrorist financing and identify suspicious and unusual transactions as well as transactions that do not have a reasonable financial purpose or if they at least contribute to the attainment of these goals.

1.6. The first requirement for the measures of prevention of money laundering and terrorist financing is that the Company does not enter into transactions or establish relationships with anonymous or unidentified persons. Legislation requires that the Company waives a transaction or the establishment of a business relationship if a person fails to provide sufficient information to identify the person or about the purpose of the transactions or if the operations of the person involve a higher risk of

money laundering or terrorist financing. Also, legislation requires the Company to terminate a continuing contract without the advance notification term if the person fails to submit sufficient information for application of CDD measures.

1.7. The Company ensures that information concerning a Customer (incl. gathered documents and details) is up to date. In the event of Customers or business relationships falling in the high risk category, the existing information will be verified more frequently than in the event of other Customers/business relationships. The respective data shall be preserved in writing or in a form that can be reproduced in writing and made available to all relevant employees who need it to perform their employment duties (management board members, account managers, risk managers and internal auditors).

1.8. The Company carries out CDD measures at the outset of any business relationship and, if necessary, where any suspicions arise subsequently on our suppliers, distributors, counterparties, agents and any person with whom the Company has an established business relationship that will involve the transfer to or receipt of funds, so the Company can ensure that there are no legal barriers to working with them before contracts are signed or transactions occur.

1.9. Various factors will determine the appropriate forms and levels of screening. The Company shall perform KYC procedure for every Customer (natural or legal entity), Representative of the Customer (an individual who is authorized to act on behalf of the Customer), Beneficial Owner of the Customer and Politically Exposed Person ("PEP") or a person connected with the PEP.

1.10. During the KYC (and registration) procedure, every Customer must provide to the Company with personal information and documents, which the Company needs to establish a portfolio of the Customer and access the risk (for more detailed risk description see Section 4 of the Policy), connected to it (see Table #1).

1.11. KYC is carried out by a third party –Simplicity Labs Pvt Ltd who is a trusted partner of the Company for collecting and processing Users data on behalf of the Company. Simplicity Labs Pvt Ltd is an experienced identity verification company that will process personal data and run KYC/AML procedures and ensure compliance with the relevant AML legislation.

1.12. For the purposes of maintaining Customers' accounts and reviewing Customers for the purposes of KYC/AML compliance, the Company will collect and process the same that Simplicity Labs Pvt Ltd will collect in the process of Customer verification (KYC) procedure, according to **Privacy Notice for Braands NFT Domain Sale**

1.13. The Company obtains all information necessary to establish to its full satisfaction the identity of each new Customer and the purpose and intended nature of the business relationship. The extent and nature of the information depends on the type of applicant (personal corporate etc.) and the expected size of the account. Therefore, the Company has categorized the Customers (and personal information) as follows:

Table #1

	Natural Person	**Legal Entity**
Low Risk	The Company shall obtain the following information: - true name and/or names used as these are stated on the official identity card or passport; - personal identification code or, if none, the date and place of birth and the place of residence or seat; - full permanent address; - telephone; - e-mail address, if any; - nationality. *The Company identifies a natural person based on the following documents:* *- a valid travel document issued in a foreign country;* *- a driving license* *The Customer's permanent address shall be verified by a recent (up to 3 months) one of the following documents:* *- a utility bill,* *- a local authority tax bill or a bank statement or* *- any other document same with the aforesaid.* *Verification of identity and current address should be sought from a reputable credit or financial institution in the applicant's country of residence. Document acceptable and provided by the Customers must be*	The Company shall obtain the following information: - the name or business name of the legal person; - the registry code or registration number and the date of registration; - the names of the director, members of the management board or - other body replacing the management board, and their authorization in representing the legal person; - the details of the telecommunications of the legal person; - the registry card of the relevant register; - the registration certificate of the relevant register, or - a document equal to the document specified above; - the full addresses of the registered office and the head offices; - the individuals that are duly authorized to operate the account and to act on behalf of the legal person; - the registered shareholders that act as nominees of the beneficial owners; - the economic profile of the legal person. - certificate of incorporation and certificate of good standing (where available).

	provided preferably in color, a copy must be clearly readable, the full document must be visible.	
Normal Risk	The Company may request the following additional information to the KYC Low Risk Customers: - about the Customer identification; - about the planned substance of the business relationship; - about the origin of the funds and wealth of the Customer and its beneficial owner; - about the underlying reasons of planned or executed transactions; - any other information in order to assist the Company to decide whether to establish or continue a business relationship;	The Company may request the following additional information: - about the Customer and its beneficial owner; - about the planned substance of the business relationship; - about the origin of the funds and wealth of the Customer and its beneficial owner; - about the underlying reasons of planned or executed transactions; - any other information in order to assist the Company to decide whether to establish or continue a business relationship. When an account has been opened, but problems of verification arise in the service relationship which cannot be resolved, the Company can close the account and return the money to the source from which it was received.
High Risk	For the High-Risk Customers, the Company ensures to gather the documents that are requested from Low and Normal risk Customers, however they shall be in a certified true copy form or provide other additional documents, as the Company may see feet and reasonable. The Company shall request, depending on the circumstances and risk profile of the Customer, additional documents and:	As an additional CDD measure, on a risk-sensitive basis, the Company shall carry out (when deemed necessary) a search and obtain information from the records of the Registrar of Companies and/or any other relevant competent authority in the legal entity's country of incorporation and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as

	- an autoportrait (“Selfie picture”); - phone call; - video call; - proofs of source of funds; and - supportive documents, notarization KYC documents, and apostilled documents. The Company may demand that a Customer make a payment from an account held in the credit or financial institution.	an operating company in the records of the appropriate authority of incorporation. The Company shall request, depending on the circumstances and risk profile of the Customer, additional documents and: - an autoportrait (“Selfie picture”); - video/phone call with the appointed/authorized person; - proofs of source of funds; and - supportive documents, notarization KYC documents of individuals, and even apostilled documents.

3. ESTABLISHING THE SOURCE OF FUNDS

2.1. The Company should follow a risk-based approach when establishing Source of Funds. The risk-based approach is that the Company is on alert to any possibility that the funds may not be from a legitimate source or are not destined for a legitimate purpose. For example, when funds are sourced from a high-risk third country with inadequate AML legislation and regime, it is appropriate to obtain more information before proceeding with any transaction. A detail/extent depends on the Customer’s money laundering and terrorist finance risks.

2.2. For the purpose of ensuring that the source of the funds is legitimate, the Company undertakes the following measures:

2.2.1. Considers the reliability of the Customer based on the information provided;

2.2.2. Questions information and/or proof documents of the source of funds that the Customer intends to invest;

2.2.3. considers the jurisdiction and the bank rating that those money are being transferred;

2.2.4. Considers whether the funds are being transferred from an account which is held in the name of the Customer or a third party.

2.3. Where the funds come from a third party, the risk is greater and further enquiries shall be made by the Company: about the relationship between the Customer and the ultimate underlying principal of the funds (i.e., the actual provider of the funds) assessing whether the purpose of the transaction is in line with the documented profile of the Customer.

2.4. The Company undertakes to ensure that the source of funds is logical and backed by supporting documentation (e.g,. a deed of sale, etc.).

3. CORPORATE GOVERNANCE AND COMPLIANCE FUNCTION

3.1. In accordance with **The Prevention of Money-Laundering Act, 2002 (PMLA)** the Company is an obliged entity responsible for the implementation of **the The Prevention Of Money-Laundering Act, 2002 (PMLA) Rule 2005** and guidelines adopted on the basis thereof.

3.2. In accordance with The prevention of Money Laundering Rules, 2005 (Section – 2 (b a) the Company is the person having specific obligations and shall appoint a person who shall be responsible for the compliance with the obligations provided for in brands.io and for the performance of legislation and instructions established on the basis of the International Sanctions Act. The position of a Compliance officer within the organizational structure of the Company allows the Compliance officer to be appointed as a person who shall be responsible for the compliance with the obligations as per the rules.

3.3. The management board of the Company appoints a Compliance officer. The functions of a Compliance officer are performed by an employee and a structural unit subordinate to the Compliance officer with the relevant duties.

3.4. The Company ensures that only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a Compliance officer may be appointed as a Compliance officer.

3.5. Only a person who works permanently in India and has the education, professional suitability, abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a compliance officer. The appointment of a Compliance officer is coordinated with the Financial Intelligence Unit ("**FIU**").

3.6. The position of a Compliance officer within the organizational structure of the Company shall allow for the performance of the requirements provided by law for the prevention of money laundering and terrorist financing. Upon establishment of the compliance officer position, the compliance officer shall be made directly accountable to the management board of the Company and made as independent of business processes as possible.

3.7. The Compliance officer's independence from business processes does not mean that the officer is prohibited to advise or train colleagues for the purpose of ensuring the compliance of the actions of the executives and employees with the requirements of **The Prevention Of Money-Laundering Act, 2002 (PMLA).**

3.8. The functions of the Compliance officer are as follows:

3.8.1. organization of collection and analysis of information referring to unusual transactions or transactions suspected of money laundering or terrorist financing in the activities of the Company (collection of information means collection of any and all suspicious or unusual notices received from the employees, contractual partners and agents of the Company, and systemizing and analysis of the information contained in them);

3.8.2. reporting to the in **Financial Intelligence Unit** - India (**FIU**-IND) the event of suspicion of money laundering or terrorist financing (notice being given in the manner agreed with the FIU-IND);

3.8.3. periodic submission of written statements on implementation of the rules of procedure to the management board of the Company; and

3.8.4. Performance of other obligations related to the fulfillment of the requirements of **The Prevention of Money-Laundering Act, 2002 (PMLA)** by the Company and training employees and applying respective control mechanisms).

3.9. The Compliance officer shall have access to the information forming the basis or prerequisite for establishing a business relationship, including any information, data or documents reflecting the identity and business activity of the Customer. The management board also grants the compliance officer the right to participate in the meetings of the management board if the compliance officer deems this necessary to perform their functions.

3.10. The contact details of the Compliance officer shall be communicated to the Financial Supervision Authority. The Compliance officer shall inform the Financial Supervision Authority within a reasonable term about the appointment of a new compliance officer or a change in contact details.

4. RISK LEVELS AND CATEGORIES

4.1. The Company shall classify Customers into various risk categories and based on the risk perception decide on the acceptance criteria for each category of Customer. Where the Customer is a prospective Customer, an account must be approved only after the relevant pre-account opening CDD and identification measures and procedures have been conducted, according to the principles and procedures set in Policy. No account shall be opened in anonymous or fictitious names.

4.2. The criteria for accepting new Customers and categorization of Customers based on their risk is described below. The Compliance Officer shall be responsible for categorizing Customers in one of the following three (3) categories based on the criteria of each category set below in the Tables #2, #3, #4 and Table #1 set above.

Table #2

RISK LEVEL	RISK DESCRIPTION

Normal	These are the Customers who do not fall under the “High Risk” or “Extra High Risk” Customers
High	The Customer is from a high-risk country; The Customer is local PEP or a person associated with a PEP; The legal person’s area of activity is associated with enhanced money-laundering risk; The legal person is situated in a country, which is listed in the list of risk countries; The legal person's activities and liability are insufficiently regulated by law, and the legality of financing of which is not easy to screen; The representative or the Beneficial Owner/Shareholder of a legal person is a local PEP or his/her family member
Extra High	The Customer is suspected to be or to have been linked with a financial offence or other suspicious activities; The Customer is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries; The representative or the Beneficial Owner/Shareholders of a legal person is a PEP or his or her family member; There is information that a legal person is suspected to be or to have been linked with a financial offence or other suspicious activities; A legal person registered outside the EEA, whose field of business is associated with a high risk of money laundering, or registered in a low tax rate country

4.3. The following Table #3, Table #4 and clause 4.4 divide risk categories into risk by Customers, by countries and by transactions:

Table #3

	Suspicious facts	**Politically exposed persons**
Risk by Customers	◉ discrepancies in provided id documents; ◉ fictitious person; ◉ stolen identity; ◉ counterfeited id document; ◉ pervious financial crime record; ◉ terrorist record;	Those who perform prominent public functions: ◉ head of state; ◉ head of government; ◉ minister and deputy or assistant minister; ◉ a member of parliament or of a similar legislative body; ◉ a member of a governing body of a political party;

	◉ wanted person; ◉ no contact phone number; ◉ not valid documents; ◉ discrepancies in provided documents for the legal person, etc	◉ a member of a supreme court, a member of a court of auditors or of the board of a central bank; ◉ an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; ◉ a member of an administrative, management or supervisory body of a state-owned enterprise; ◉ a director, deputy director and member of the board or equivalent function of an international organisation, except middle-ranking or more junior officials

Table #4

	Country of residence/ nationality is a country with prohibition/ restriction on crypto currencies	**Resident/Citizen of the High Risk countries**	**Low Tax or Tax-free countries**
Risk by countries	◉ Afghanistan; ◉ Algeria; ◉ American Samoa; ◉ Bangladesh; ◉ Bolivia; ◉ China; ◉ Democratic People's Republic of Korea; ◉ Egypt; ◉ Ethiopia; ◉ Macedonia; ◉ Iran; ◉ Iraq;	◉ Bahrain; ◉ Yemen; ◉ Jordan; ◉ Kuwait; ◉ Lebanon; ◉ Libya; ◉ Mali; ◉ Mauritania; ◉ Nigeria; ◉ Oman; ◉ Somalia; ◉ Serbia; ◉ Sudan; ◉	United Arab Emirates; Oman; Bahrain; Qatar; Saudi Arabia; Kuwait; Bermuda; Cayman Islands; The Bahamas; Brunei; Vanuatu; Anguilla; Belize; Costa Rica; Guatemala; Panamá; Nicaragua.

	◉ Kyrgyzstan; ◉ Pakistan; ◉ Palestine; ◉ Qatar; ◉ Saudi Arabia; ◉ Syria; ◉ Morocco; ◉ Nepal; ◉ United States Of America; ◉ Vanuatu; ◉ Zambia.	Turkey; Ethnic Groups Of Caucasus Belonging To Russian Federation (Chechens, Etc.); Trinidad & Tobago.	

4.4. The Company shall inspect any outstanding transaction (Section 6 - detection of suspicious transactions), which include but is not limited to the:

4.4.1. large transactions that do not correspond to Customer's source of funds and/or source of wealth;

4.4.2. transactions to offshore or shell bank (financial institution that does not have a physical presence in any country);

4.4.3. executing payment via non-licensed payment institution;

4.4.4. large daily movements of fiat or virtual money, etc.

5. NOT ACCEPTABLE CUSTOMERS

5.1. The following list predetermines the type of Customers who are not acceptable for establishing a business relationship or an execution of an occasional transaction with the Company:

5.1.1. shell banks;

5.1.2. Customers from the jurisdictions which are being banned by internal policies from the company or international sanctions;

5.1.3. Customers who were identified as the persons subject to International Sanction Act;

5.1.4. EU Sanctions;

5.1.5. sanctions administered by the Office of Financial Sanctions Implementation, Sanctions administered by the Office of Foreign Assets Control;

5.1.6. Customers who were identified as the persons subject to the UN Sanctions;

5.1.7. the Company suspects money laundering or terrorist financing;

5.1.8. any other that the Company considers risky to its business or suspicious in regards to money laundering and terrorist financing;

5.1.9. the Company is prohibited to establish a business relationship or make a transaction with a person whose capital consists of bearer shares or other *bearer securities to the extent of more than 10 percent.*

5.2. The Company will not accept as Customers, persons or entitled from Afghanistan, Angola, Algeria, Bahamas, Bangladesh, Bolivia, Botswana, Burma (Myanmar), Burundi, Cambodia, Chad, Gvineja, Côte D'ivoire, Crimea (Ukraine region), Cuba, Democratic People's Republic of Korea, Egypt, Equatorial Guinea, Eritrea, Ghana, Guinea Bissau, Guyana, Iceland, Iran, Iraq, Haiti, Lao PDR, Lebanon, Libya, Mali, Mongolia, Morocco, Myanmar, Nepal, Nicaragua, North Macedonia, Pakistan, Panama, Qatar, Saudi Arabia, Somalia, South Sudan, Sudan, Syria, Trinidad and Tobago, Uganda, United States, Vanuatu, Venezuela, Yemen, Zimbabwe and other countries and jurisdictions, where these services cannot be provided by legislation countries.

5.3. Persons or entities from jurisdictions where a particular license or permit is required will not be accepted as Customers if the Company has not received such a permit or license.

6. SUSPICIOUS TRANSACTIONS

6.1. Where the Company identifies an activity or facts whose characteristics refer to the use of criminal proceeds or terrorist financing or to the commission of related offences or an attempt thereof or with regard to which the obliged entity suspects or knows that it constitutes money laundering or terrorist financing or the commission of related offences (the "suspicious transaction"), the Company will report such case to the FIU-IND immediately, but not later than within two working days.

6.2. A suspicious transaction will often be one which is inconsistent with a Customer's known, legitimate business or personal activities or with the normal business of the specific account. The Company shall ensure that it maintains adequate information and knows enough about its Customers' activities in order to recognize on time that a transaction or a series of transactions is unusual or suspicious.

6.3. In order to identify suspicious transactions, the Company's Compliance officer shall perform the following activities:

6.3.1. monitor on a continuous basis any changes in the Customer's financial status, business activities, type of transactions etc.

6.3.2. receive and investigate information from the Company's employees, on suspicious transactions which creates the belief or suspicion of money laundering.

6.3.3. evaluate and check the information received from the employees of the Company, with - reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors;

6.3.4. if, as a result of the evaluation described above, the Compliance Officer decides to disclose this information to FIU-IND, then he prepares a written report, which he submits to the Management Board;

6.3.5. if as a result of the evaluation described above, the Compliance Officer decides not to disclose the relevant information to the Unit, then he fully explains the reasons for his decision to the Management Board.

7. TRANSACTIONS WITH POLITICALLY EXPOSED PERSONS

7.1. In a situation where a person participating in a transaction made in economic or professional activities, a person participating in a professional act, a person using a professional service, a Customer or their beneficial owner is a politically exposed person, a family member of a politically exposed person or a person known to be a close associate of a politically exposed person, the Company applies the following due diligence measures in addition to the due diligence measures provided for in subsection of the as per the mutual signed countries

7.1.1. obtains approval from the senior management to establish or continue a business relationship with the person;

7.1.2. applies measures to establish the origin of the wealth of the person and the sources of the funds that are used in the business relationship or upon making occasional transactions;

7.1.3. monitors the business relationship in an enhanced manner.

7.2. Where a politically exposed person no longer performs important public functions placed upon them, the Company must at least within 12 months take into account the risks that remain related to the person and apply relevant and risk sensitivity-based measures as long as it is certain that the risks characteristic of politically exposed persons no longer exist in the case of the person.

8. REPORTING TO FINANCIAL INTELLIGENCE UNIT

8.1. If upon performance of economic or professional activities or professional operations or provision of professional services, the Company identifies an activity or circumstances which might be an indication of money laundering or terrorist financing or an attempt thereof or in the event of which the Company has reason to suspect or knows that it is money laundering or terrorist financing, the Company shall immediately, but not later than within two working days from identifying the act or circumstances or from the rise of the suspicion, notify the FIU-IND thereof.

8.2. The Company shall immediately, but not later than within two working days of executing the transaction, notify the FIU-IND of any transaction where the financial

obligation exceeding Rs. 10 Lac INR ((Circular DBOD.BP.BC.57/21.01.001/95 dated May 4,1995) or an equal amount in another currency is performed in cash, regardless of whether the transaction is made in a single payment or several related payments.

8.3 The Company immediately submits to the FIU-IND all the information available, which the FIU-IND requested in its enquiry.

8.4. Where the Company suspects or knows that terrorist financing or money laundering or related criminal offences are being committed, the making of the transaction or professional act or the provision of the official service must be postponed until the submission of a report. Where the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible money laundering or terrorist financing, the transaction or professional act will be carried out or the official service will be provided and a report will be submitted the FIU-IND thereafter.

8.5. In case of any such suspicion, the Company may suspend and/or postpone the transaction until the report, as per this paragraph, is made. If such suspension and/or postponement may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible money laundering or terrorist financing, the transaction or professional act will be carried out or the service will be provided and a report will be submitted the FIU-IND thereafter.

8.6. If, as a result of application of due diligence measures the Company identifies a subject of the financial sanction or that the transaction or act which is planned or carried out by them violates financial sanctions, or if additional information obtained upon application of due diligence measures does not enable to identify it, as well as in the case of the suspicion of violation of financial sanctions the Company is not allowed to establish a business relationship or enable the making of an occasional transaction or the making of a transaction in a business relationship.

8.7 If, as a result of application of due diligence measures the Company identifies a subject of the financial sanction or that the transaction or act which is planned or carried out by them violates financial sanctions, or if additional information obtained upon application of due diligence measures does not enable to identify it, as well as in the case of the suspicion of violation of financial sanctions, the Company shall inform the FIU-IND thereof and of the financial sanction applied.

8.8. The report is submitted via the registered Indian post to the FIU –IND or via ctrcell[at]fiuindia[dot]gov[dot]in (For Reporting Entity / Principal Officer registration related queries) . The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.

8.9. The Company will not inform the person, its beneficial owner, representative or third party about a report submitted on them to the FIU, a plan to submit such a report or the occurrence of reporting as well as about a precept made by the FIU-IND or about the commencement of criminal proceedings. After a precept made by the FIU-IND has been complied with, the Company may inform a person that the

FIU-IND has restricted the use of the person's account or that another restriction has been imposed.

8.10. The prohibition of informing is not applied upon submission of information to:

8.10.1. Competent supervisory authorities and law enforcement agencies;

8.10.2. Credit institutions and financial institutions in between themselves where they are part of the same group;

8.10.3. Institutions and branches that are part of the same group where the group applies group-wide procedural rules and principles in accordance with relevant laws;

8.10.4. a third party who operates in the same legal person or structure as an obliged entity who is a notary, enforcement officer, bankruptcy trustee, auditor, attorney or other legal service provider, provider of accounting services or provider of advisory services in the field of accounting or taxation and whereby the legal person or structure has the same owners and management system where joint compliance is practiced.

9. RELIEF FROM LIABILITY

9.1. The Company, its employee, representative or a person who acted in its name shall not, upon performance of the obligations arising from the **The Prevention Of Money-Laundering Act, 2002 (PMLA)** be liable for damage arising from failure to enter into a transaction or failure to enter into a transaction by the due date if the damage was caused to the person participating in the transaction made in economic or professional activities in connection with notification of the FIU-IND of the suspicion of money laundering or terrorist financing in good faith, or for damage caused to a Customer or a person participating in a transaction entered into in economic or professional activities in connection with cancellation of a contract.

9.2. The performance in good faith of the notification obligation arising from **The Prevention Of Money-Laundering Act, 2002 (PMLA) & PMLA Rules 2005** and communication of relevant data by the Company is not deemed infringement of the confidentiality requirement provided by law or contract and no liability provided by legislation or contract is imputed with regard to the person who performed the notification obligation for disclosure of the information.

9.3. Taking into account its size and nature of activities, the Company establishes an appropriate system of measures ensuring that the employees and representatives of the Company who report of a suspicion of money laundering or terrorist financing or of a violation of the **The Prevention Of Money-Laundering Act, 2002 (PMLA)** are able to do so anonymously and are protected from being exposed to threats or hostile action by other employees, management body members or Customers of the Company, in particular from adverse or discriminatory employment actions.

10. COOPERATION AND EXCHANGE OF INFORMATION

10.1. The Company cooperates with supervisory and law enforcement authorities in preventing money laundering and terrorist financing, thereby communicating information available to the Company and replying to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation. For any relevant requests please contact us at compliance@braands.io

Please note that in case you represent the law enforcement agency outside of the Republic of India, procedure under the Mutual Legal Assistance Treaty may apply.

ANNEX #1

To the Anti-Money Laundering Policy

CUSTOMER CLASSIFICATION GUIDE

This Customers Classification Guide ("**Guide**") prepared by the Braandsio Internet Private Limited , a company incorporated under the laws of India under registered number U72900HR2022PTC107422, having legal and business address at: 145, 1st Floor, JMD Megapolis, Sector-48, Gurgaon, Haryana, India, 122018 (the "**Company**"), website https://braands.io

This Guide prepared according to the prevention of Money-Laundering Act, 2002 (15 of 2003), rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the reporting entities, and called "The Prevention of Money-Laundering (Maintenance of Records Rules), 2005"

The Table below sets out the classification of the Company's customers based on the amount of transaction(s) (in euros) made by the customers in one calendar year. The number and type of documents required to initiate the Know Your Client procedure depends on the type of customer (e.g. transaction amount, legal entity or individual).

The list of documents stated in the Table below is not exhaustive and additional documentations might be required on a case-by-case basis depending on a risk-based approach.

"Customers Classification" Table

LEGAL ENTITIES			
	Low Risk (up to $5000)	**Normal Risk** (from $5000 to	**High Risk** (from $12000 and

		$12,000)	more)
Required Documents	• business name of the legal person; • the registry code; • registered Company Address (Street, House Number, Postcode/Zip Code, City, Country); • website; • email; • activities of the company.	All documents mentioned in the “Low Risk” section plus: • register of Directors signed by Director (*not older than 6 months*); • register of Shareholders/Members signed by Director (*not older than 6 months*); • official identity card or driver license, utility bill (*not older than 3 months*) for all Directors and all ultimate beneficial shareholders (*having more than 25% of ownership in the company*).	All documents mentioned in the “Low Risk” and Normal Risk sections plus: • proofs of source of funds; • phone/video call with the appointed/authorized person; • supportive documents, notarization KYC documents, and apostilled documents.
NATURAL PERSONS			
	Low Risk (up to $5000)	**Normal Risk** (from $5000 to $12,000)	**High Risk** (from $12000 and more)
Required Documents	• Official identity card or driver license (**Note** *that driver license must meet the requirements provided for in subsection 1 of §4 of the Indian Identity Documents Act*); • personal identification code or, if	All documents mentioned in the “Low Risk” section plus: • a utility bill; • a local authority tax bill or a bank statement; or • any other document same with the aforesaid. **Note** *that permanent address shall be verified by recent (up to 3 months) documents.*	All documents mentioned in the “Low Risk” and Normal Risk sections plus: • proofs of source of funds; • phone/video call; • supportive documents, notarization KYC documents, and apostilled documents.

	none, the date and place of birth and country of residency; • full permanent address; • nationality; • telephone; • email.		

All documentation provided must be in the English language. If the documents need to be translated, the translation should be dated, signed, and certified by an independent person of proven competence, confirming the document to be a faithful translation of the original.

ANNEX-2

Customer Identification Procedure

Features to be verified and documents that may be obtained from customers

Features	**Documents**
Accounts of individuals - Legal name and any other names used - Correct permanent address	(i) Passport (ii) PAN card (iii) Voter's Identity Card (iv) Driving license (v) Identity card (subject to the bank's satisfaction) (vi) Letter from a recognized public authority or public servant verifying the identity and residence of the customer to the satisfaction of bank (i) Telephone bill (ii) Bank account statement (iii) Letter from any recognized public authority (iv) Electricity bill (v) Ration card (vi) Letter from employer (subject to satisfaction of the bank) (any one document which provides customer information to the satisfaction of the bank will suffice)
Accounts of companies - Name of the company - Principal place of business - Mailing address of the company	(i) Certificate of incorporation and Memorandum & Articles of Association (ii) Resolution of the Board of Directors to open an account and identification of those who have authority to operate the account (iii) Power of Attorney granted to its managers, officers or employees to transact business on its behalf (iv)

- Telephone/Fax Number	Copy of PAN allotment letter (v) Copy of the telephone bill
Accounts of partnership firms - Legal name - Address - Names of all partners and their addresses - Telephone numbers of the firm and partners	(i) Registration certificate, if registered (ii) Partnership deed (iii) Power of Attorney granted to a partner or an employee of the firm to transact business on its behalf (iv) Any officially valid document identifying the partners and the persons holding the Power of Attorney and their addresses (v) Telephone bill in the name of firm/partners
Accounts of trusts & foundations - Names of trustees, settlers, beneficiaries and signatories - Names and addresses of the founder, the managers/directors and the beneficiaries - Telephone/fax numbers	(i) Certificate of registration, if registered (ii) Power of Attorney granted to transact business on its behalf (iii) Any officially valid document to identify the trustees, settlers, beneficiaries and those holding Power of Attorney, founders/managers/ directors and their addresses (iv) Resolution of the managing body of the foundation/association (v) Telephone bill

2.16 Maintenance of records of transactions/Information to be preserved/Maintenance and preservation of records/Cash and Suspicious transactions reporting to Financial Intelligence Unit- India (FIU-IND)

Government of India, Ministry of Finance, Department of Revenue, vide its notification dated July 1, 2005 in the Gazette of India, has notified the Rules under the Prevention of Money Laundering Act (PMLA), 2002. In terms of the said Rules, the provisions of PMLA, 2002 came into effect from July 1, 2005. Section 12 of the PMLA, 2002 casts certain obligations on the banking companies in regard to preservation and reporting of customer account information. Banks are, therefore, advised to go through the provisions of PMLA, 2002 and the Rules notified there under and take all steps considered necessary to ensure compliance with the requirements of Section 12 of the
Act ibid.

(i) Maintenance of records of transactions

Banks should introduce a system of maintaining proper record of transactions prescribed under Rule 3, as mentioned below:

a) all cash transactions of the value of more than Rupees Ten Lakh or its equivalent in foreign currency;

b) all series of cash transactions integrally connected to each other which have been valued below Rupees Ten Lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of

such transactions exceeds Rupees Ten Lakh;

c) all cash transactions where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security or a document has taken place facilitating the transaction and

d) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.