



ANTI – MONEY LAUNDERING POLICY

Krypto (Inventphile Ventures Pvt Limited) and/or its subsidiaries and affiliates (hereinafter referred to as “Company” which term shall refer to and include its owners, directors, investors, employees or other related parties) is a private limited company incorporated under the laws of India. Persons availing of the any services from Company, or engaging in any transactions on any digital/non digital platform provided or operated by Company, directly or indirectly, are referred to herein, as “Users”.

This is an agreement between Company and User, which is binding on the User. All Users are required to comply with the terms of this agreement at all times, and any instance of non-compliance may result in the termination of such User’s accounts on the Company platform, and in appropriate reporting of the circumstances of such non-compliance and such termination to the relevant statutory authorities. Users are required to strictly comply with the terms contained herein, which forms part and parcel of the User [Terms of Use]. Terms not defined herein shall carry the same meaning as in the Terms of Use, and in the absence thereof, to general usage and parlance.

Users are required to read, review, understand and then agree to the terms hereunder for using or availing of the Company Services, before clicking the “I Accept” option.

This Anti-Money Laundering Policy (herein after referred to as the “AML Policy”) supersedes and replaces any and all prior oral or written understandings or agreements between Company and the User with respect to the AML Policy.

I. DEFINITIONS

All terms defined in the Terms of Service and the Privacy Policy will carry the same meaning, force and effect in this AML Policy.

a) “Applicable Law” means all laws in force for the time being within the territory of India, including (but not restricted to) the Prevention of Money Laundering Act 2002 (“PMLA”), the Prevention of Money Laundering (Maintenance of Records) Rules 2005 (“PML Rules”), and the Reserve Bank of India’s (“RBI”) Master Direction on Know Your Customer Rules (“KYC Rules”), as updated from time to time;

b) “Designated Director” means a managing director or whole-time director of Company who has been appointed and authorized to administer Company’s anti-money laundering measures, in accordance with the PMLA;

c) “Principal Officer” means the officer appointed by Company to administer Company’s anti-money laundering measures, in accordance with the PMLA;

d) “Senior Management” means such directors, officers or other personnel of Company as are specifically designated to monitor and ensure know-your-customer compliance and the operation of Company’s internal audit systems;

e) “Suspicious Transaction” means a transaction, whether or not made in cash which, to a person acting in good faith:

- i. Give rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified in the Schedule to the PMLA, regardless of the value involved; or
- ii. appears to be made in circumstances of unusual or unjustified complexity; or
- iii. appears to have no economic rationale or bona fide purpose; or
- iv. gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;



Explanation. —Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism

II. MAINTENANCE OF RECORDS

a) Company shall maintain a record of, and has evolved an internal mechanism to detect, the following:

i. Details pertaining to User transactions, including but not limited to:

- a. the nature of the transactions;
- b. the amount of the transaction and the currency in which it was denominated;
- c. the date on which the transaction was conducted; and
- d. the parties to the transaction.

ii. All details for the following categories of User transactions, separately from those recorded under (i) above:

a. User transactions of value of at least INR 10,00,000 (Indian Rupees Ten lakh), or its foreign currency equivalent; and

b. User transactions that are connected to each other and that take place within a month of each other, with a monthly aggregate of at least INR 10,00,000 (Indian Rupees Ten lakh), or its foreign currency equivalent; and

iii. All Suspicious Transactions by way of deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of:

a. cheques including third party cheques, pay orders, demand drafts, or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits; or

b. transfers from one account within the same banking company, financial institution and intermediary, including to and from Nostro and Vostro accounts; or

c. any other mode in whatsoever name it is referred to;

iv. credits or debits into or from any non-monetary accounts such as demat account, security account in any currency maintained by Company;

v. money transfer or remittances in favor of own Users or non-Users from India or abroad and to third party beneficiaries in India or abroad including transactions on its own account in any currency by any of the following:

- a. demand drafts, or
- b. telegraphic or wire transfers or electronic remittances or transfers, or
- c. internet transfers, or
- d. Automated Clearing House remittances, or
- e. any other mode of money transfer by whatsoever name called;

vi. letters of credit, standby letters of credit, guarantees, comfort letters, solvency certificates and any other instrument for settlement and/or credit support;



vii. collection services in any currency by way of the collection of bills, cheques, instruments or any other mode of collection in whatsoever name it is referred to.

III. PROCEDURE AND MANNER OF MAINTAINING INFORMATION

a) Company will maintain hard and soft copies of the above-mentioned records of Transactions in accordance with the procedure and manner, as may be specified under applicable laws or regulations, from time to time.

b) In addition to the above, Company shall maintain records of transactions, as per its prevailing processes.

IV. DISCLOSURE OF RECORDS

a) Company may be required and / or directed to cooperate and aid the government and / or law enforcement authorities, police, investigating agencies, or Tribunals and Courts within the territory of India or from outside the said territory.

b) In such cases, subject to applicable laws with respect to data protection, Company shall be entitled to disclose any information about the User that is in its possession or control, including to government or law enforcement officials, police, investigating agencies, Tribunals and Courts within the territory of India.

c) In particular, Company shall be entitled to initiate processes and disclosures, including but not limited to the following circumstances:

- i. information pertaining to or in pursuance of claims and legal process (such as summons / warrants);
- ii. to protect Company's property, rights, and safety and the property, rights, and safety of a third party or the public in general;
- iii. to identify and stop any activity that Company considers illegal, unethical, or legally actionable.

d) Company may, if so required under applicable Law, disclose the following information to the Director of the Financial Intelligence Unit-India, as appointed under the PMLA:

- i. Name, designation and address of the Designated Director, the Principal Officer and all Senior Management;
- ii. User transactions listed in II(a)(ii) above by the 15th day of each succeeding month, or more frequently if so instructed by the authorities;
- iii. User transactions listed in II(a)(iii) within seven working days of being satisfied that the transaction in question is suspicious in nature, or more frequently if so instructed by the authorities.

e) Company also compiles records and audit and compliance notes to determine the efficacy of its internal audit systems on an ongoing basis, and such notes are submitted to Company's audit committee on a quarterly basis for this purpose.

V. VERIFICATION AND DUE DILIGENCE PROCESS FOR USERS

Company's User due diligence and KYC incorporates relevant requirements prescribed under Applicable Law, and has been approved by Company's board of directors and Senior Management. Users are required to comply with the policy, as follows:

a) Every User is compulsorily required to submit at the time of opening an account, documents and details as set out in this policy. Company is required to identify the said User based on the said documentation whenever an account is opened by a User.



b) Company shall determine the identity of the User and shall take all reasonable steps to verify Users identity. An account will not be opened for a User if reliable customer due diligence cannot be conducted for such User.

c) If Company engages the services of a third party to carry out the User identification process, Company will ensure that:

- i. Company obtains the User due diligence carried out by such third party within two days;
- ii. adequate steps are taken to ensure that copies of any part of the User due diligence will be made available by such third party without delay, upon request;
- iii. it is satisfied that such third party is regulated, supervised or monitored by, and complies with due diligence and record-keeping requirements prescribed under, the PMLA;
- iv. such third party is not based in a high-risk jurisdiction;
- v. no decision-making functions of Company are outsourced to such third-party;
- vi. Users are not required to furnish any additional copies of officially valid documents to such third-party;
- vii. Company itself is ultimately responsible for User due diligence; and
- viii. Company will comply with all other requirements that may be prescribed under all relevant anti-money laundering regulations.

d) At the time of onboarding, all new Users are required to submit copies of: (i) their PAN card; (ii) bank account details, including account number, branch details, IFSC code, account name, and bank name; and (iii) Aadhaar card. Company will carry out e-KYC authentication for a User using their Aadhaar number, if such User has provided explicit authorization for the UIDAI to release their personal information through biometric authentication.

e) Company will determine whether a User is acting on behalf of a beneficial owner, and will take all necessary steps to identify such beneficial owner. If the User

f) Users are not permitted to act on behalf of another User, and can only transact on the Company platform on their own account, with their own funds, and for their own benefit.

g) Users are not permitted to open any of the following:

- i. an anonymous account;
- ii. an account under a fictitious name; or
- iii. an account on behalf of other persons whose identity is undisclosed or unverifiable.

h) No accounts will be opened by Company for any User who appears on the United Nations Security Council's ISIL (Da'esh) & Al-Qaida Sanctions List, or on its 1988 Sanctions List.

i) Where the User is an individual, the User shall submit one copy of an officially valid document containing details of his/her permanent address or addresses, current address or addresses, and one copy of his/her recent photograph, which may be a passport, a driving license, PAN card, voter's identity card, job card issued by the NREGA and signed by an official of the state government, and/or a letter issued by the UIDAI containing the name, address and Aadhaar number of such User.

j) Where the User is a company, it shall submit to Company the following: (i) Certificate of incorporation; (ii) Memorandum and Articles of Association; (iii) a resolution from the Board of Directors for trading in cryptocurrencies, and providing power of attorney to its managers, officers or employees to transact on its behalf; (iv) Aadhaar number; (v)



the PAN, driving license, voter's identity card, NREGA job card, or UIDAI letter containing name, address and Aadhaar number, of the managers, officers or employees holding a power-of- attorney to transact on the User's behalf; and other documents as may be requested.

k) Where the User is a partnership firm, it shall submit to Company one certified copy of the following documents:

(i) registration certificate; (ii) partnership deed; and (iii) authorization letter for trading in cryptocurrencies; (iv) Aadhaar number; (v) the PAN, driving license, voter's identity card, NREGA job card, or UIDAI letter containing name, address and Aadhaar number, of the person holding a power-of-attorney to transact on the User's behalf; and other documents as may be requested.

l) Where the User is trust, it shall submit to Company one certified copy of the following documents: (i) registration certificate; (ii) trust deed; and (iii) authorization letter for trading in cryptocurrencies; (iv) Aadhaar number; (v) the PAN, driving license, voter's identity card, NREGA job card, or UIDAI letter containing name, address and Aadhaar number, of the person holding a power-of-attorney to transact on the User's behalf; and other documents as may be requested.

m)Where the User is a juridical person, it shall submit to Company one certified copy of the following documents:

(i) document showing the name of the person authorized to act on behalf of the User; (ii) the PAN, driving license, voter's identity card, NREGA job card, or UIDAI letter containing name, address and Aadhaar number, of the person holding a power-of-attorney to transact on the User's behalf; ; and other documents as may be requested.

n)Where the User is a juridical person, Company shall verify that any person purporting to act on behalf of such User is so authorized and shall verify the identity of that person.

o)Company may, if so, required under applicable Law, file know-your-customer records with the Central Registry of Securitization Asset Reconstruction and Security Interest of India ("CERSAI") within 3 days of onboarding a new User, and may communicate a User's KYC Identifier once it has been assigned by CERSAI for such User.

p)Company will not use the KYC records of any User for any purpose other than the verification of identity or address, and cannot transfer such records to any third party without prior authorization of such User, or the Director or other regulator appointed under the PMLA. All information collected from Users is treated as confidential, and will not be used for cross-selling. The information collected will be as non-intrusive as possible, and requests for any information that is not mandatory will be labelled as optional.

q)Users who are politically exposed persons ("PEPs") can only open an account on the Company platform under the following circumstances:

- i. Company is able to gather sufficient information about the sources of funds of the family members and close relatives of such PEP;
- ii. the decision to open an account for the PEP on the Platform is taken by Senior Management, and Senior Management may decline to open such an account for any reason that it deems suitable, at its sole discretion;
- iii. the account of the PEP will be subjected to enhanced, ongoing monitoring, and such User is required to consent to such monitoring; and
- iv. if an existing User becomes a PEP at any point, Senior Management is required to provide its approval before such User's relationship with Company can be continued, and Senior Management may decline to open such an account for any reason that it deems suitable, at its sole discretion.

VI. ONGOING DUE DILIGENCE MEASURES FOR TRANSACTIONS ON THE COMPANY PLATFORM



- a) Company shall exercise ongoing due diligence with respect to the business relationship with every User and closely examine the transactions in order to ensure that they are consistent with their knowledge of the User, his business and risk profile and where necessary, the source of funds.
- b) Company will also review its due diligence measures and undertake measures to re-verify the identity of a User and obtain further information on a User's activities, if Company has any suspicions of money laundering or the financing of terrorism.
- c) Company will periodically verify the identity of all Users to determine whether there are any matches with any names appearing on any of the RBI's sanctions lists.
- d) All due diligence undertaken by Company is documented, designed to consider all relevant risk factors in determining overall risk and the appropriate mitigatory measures, is kept up to date; and will always be available to the relevant authorities and self-regulating bodies.
- e) Company will maintain physical copies of all identity documents of Users, after filing such documents and records with CERSAI for KYC purposes (if so required under applicable Law).
- f) Company will verify the identity of Users while carrying out transactions worth at least INR 50,000 (Indian Rupees Fifty thousand), whether through a single transaction or a series of connected transactions. If Company has reason to believe that a User is intentionally structuring a transaction into a series of transactions, below the threshold of INR 50,000 (Indian Rupees Fifty thousand), it will undertake separate customer identification procedures.
- g) In the event that it is brought to the attention of Company, that a particular User or account is maintained under a fictitious name, Company has the full right and authority to terminate and close such an account with immediate effect and without prior notice to the User.
- h) If Company doubts the adequacy or veracity of previously obtained customer identification data, Company shall review the due diligence measures including verifying again the identity of the User and obtaining information on the purpose and intended nature of the business relationship, as the case may be. Company may also undertake customer identification procedures if third-party products are being sold on the Company platform, with dues of such sale exceeding INR 50,000 (Indian Rupees Fifty thousand)
- i) Once a User has participated in transactions of a total value of at least INR 50,00,000 (Indian Rupees Fifty lakh) over the course of his/her engagement with the Company platform, Company will initiate a process of additional due diligence by seeking the following documentation from such Users:
- i. a customer declaration form, stating that all cryptocurrencies and all funds used by such User on the Company platform are sourced through legitimate channels, and containing other details in relation to the User;
 - ii. bank statements for such Users over the previous three months;
 - iii. a certificate from a chartered accountant, with details in relation to the financial soundness of the User and the User's compliance with the PMLA and Foreign Exchange Management Act 1999; and
 - iv. documents for the physical verification of identity and address for such User.
- j) Company will classify all Users as high-risk, medium-risk or low-risk, and will periodically update the KYC records for all Users as follows:
- i. once every two years for high-risk Users;
 - ii. once every eight years for medium-risk Users; and



iii. once every ten years for low-risk Users.

k) Once a User has participated in transactions of a total value of at least over the course of his/her engagement with the Company platform, or deposits or transacts in an amount of at least INR 50,00,000 (Indian Rupees Fifty lakh) on the Company Platform, Company will also conduct 'chain analysis' to identify the relevant public address for such User and earmark such User as either as 'high risk', 'medium risk', or 'low risk' based on parameters such as the use of cryptocurrencies by such Users at online gambling websites, darknet websites, etc. This limit of INR 50,00,000 (Indian Rupees Fifty lakh) may be revised by Company from time to time, based on Company's determination of appropriate thresholds in accordance with ongoing compliance measures, and if so required under applicable Law.

l) Company will, in particular, monitor the following categories of transactions, and will conduct due diligence on an ongoing basis on them:

i. large, complex transactions, including those with unusual patterns that are inconsistent with a User's normal / expected level of activity, without an apparent economic rationale or legitimate purpose; and

ii. transactions that involve high account turnover, inconsistent with the size of the balance ordinarily maintained by a User.

m) As Users are not face-to-face customers of Company, Company may be required to undertake enhanced due diligence, including certification of all documents provided by the Users, calling for additional documents whenever necessary, and requiring that the first payments made by such Users be effected through the User's KYC-compliant account with a bank. Any such requirements, as may be imposed under Applicable Law, will be incorporated into this AML Policy, and Company reserves the right to update the AML Policy for this purpose.

n) Company's staff are trained in Company's due diligence and anti-money laundering measures, as well as all requirements prescribed under Applicable Law for this purpose, and may be contacted if any User has questions or concerns about any of the measures contained in this AML Policy.

VII. OBLIGATION ON THE PART OF THE USER

a) The User hereby agrees and undertakes to not indulge, assist, abet and encourage in any manner whatsoever, in any activity involving money laundering or financing of any illegal or unlawful activities.

VIII. RETENTION OF RECORDS

Company shall maintain such records of the identity of Users in hard and soft copies in a manner, as may be specified under applicable laws or regulations, from time to time, and in the absence thereof, from the date of cessation of the transactions between the User and Company for a period of

a) Ten years for ordinary transactions; and

b) Twelve years in case of Suspicious Transactions

IX. NOTICES

a) Any notice or other communication provided for in this Agreement shall be sent only through electronic mail. User hereby agrees to receive electronic or any other form of communication and notifications from Company. Email messages sent over the Internet are not always secure and Company is not responsible or liable for non-receipt of such communication by User. Once the email is dispatched by Company, it shall be deemed to have been served on the User. Company shall be deemed to have received communications from the User only upon actual receipt into the Inbox of the account of the person to whom such communication is addressed and acknowledged. Company shall not be liable or



responsible for non-receipt of communications or for any damages incurred by the result of sending email messages over the Internet.

b) All communications to Company shall be at info@letsrypto.com. Company shall ensure that any change or modification to the same is uploaded on the Company Website.

c) All communications to User shall be at the electronic mail address provided by User, as part of the KYC norms. User shall ensure that any change in the electronic mail address or communication option is duly intimated to Company.

X. GOVERNING LAW & JURISDICTION

a) This Agreement shall be governed by and construed in accordance with the laws of India.

b) The parties agree to irrevocably submit to the exclusive jurisdiction of the courts in Ahmedabad for the resolution of any disputes arising from this Agreement or in connection therewith or pursuant thereto.

XI. SUCCESSORS

This Agreement shall bind and inure to the benefit of the parties, and their respective successors and permitted assigns.

XII. SEVERABILITY

a) The invalidity or unenforceability of any provision of this Agreement shall not in any way affect, impair or render unenforceable this Agreement or any other provision contained herein, which shall remain in full force and effect.

b) This Agreement shall be considered divisible as to such provision, which is deemed to be invalid or unenforceable and the remainder of this Agreement shall be enforceable and binding on the Parties.

XIII. WAIVER

No provision of this Agreement may be waived or changed except by a writing signed by the party against whom such waiver is sought to be enforced. The failure or omission by either party at any time to enforce or require strict or timely compliance to any provision of this Agreement shall not affect or impair that provision or any other provision in any way or the rights of such party hereof, to avail itself of the remedies it may have in respect of any subsequent breach of that or any other provision.

XIV. RECITALS

The Recitals, Schedules and Annexures in this Agreement shall form part of this Agreement and the contents thereof shall be read into this Agreement. Headings are for the purpose of easy reference and shall not affect the meaning or interpretation of this Agreement.

XV. ENTIRETY

This Agreement, and the other agreements contemplated hereby, constitute the entire agreement.

XVI. GOVERNMENT APPROVALS

a) This Agreement is subject to confirmation by the Government of India of the legality of facilitating the dealing in Cryptocurrencies (including bitcoins), and in the event that the Government of India was to hold that transactions involving cryptocurrencies are invalid or illegal in India, this Agreement shall stand automatically terminated without further notice to User.

b) Company has given full disclosure of the current Government in relation to Company's business and regulatory status, and has sought discussions with the Government with respect to Cryptocurrencies including bitcoins in India and the risk



involved in dealing with or investing in the same. The current regulatory status and permissibility of the use of cryptocurrencies, including bitcoins, in India is unclear. The User is deemed to have understood, agreed to and accepted the risk and costs of such investment.

XVII. DESIGNATED DIRECTOR AND PRINCIPAL

Company shall appoint a Principal Officer and a Designated Director, and will designate Senior Management as required under Applicable Law, along with setting up a compliance team, who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

XVIII. MODIFICATIONS

a) These terms may be periodically reviewed and revised. The revised terms will be uploaded on the Company Website and will reflect the modified date of the terms. The User is required to periodically visit the website and review terms and any changes thereto.

b) Continued use of the Company Services constitutes the agreement of User to the terms contained herein and any amendments thereto.

c) This agreement or the responsibilities or benefits arising therefrom cannot be assigned by User save and except with the prior written consent of Company.

XIX. MISCELLANEOUS

All other provisions of the Company Terms of Service shall be read into this policy and shall form part hereof, including Governing Laws and Jurisdiction, notices, severability, assignment and such or other provisions.