KYC POLICY

ParaaCrypto is a pioneer platform dedicated to providing secure and innovative cryptocurrency trading and investment solutions.

COMPANY DETAILS (herein referred to as “ParaaCrypto” or “Company”), CIN U62099CT2024PTC016430, a Legally Company under Indian Company Laws Laws, having it registered place of busines at Raipur, Chattisgarh operates the Platform.

THIS KYC POLICY ("POLICY") CONSTITUTES A LEGAL AGREEMENT BETWEEN YOU, AS A USER OF THE ONLINE PLATFORMS, AND US. BY CREATING AN ACCOUNT OR BY VISITING/ACCESSING THE PLATFORMS IN ANY CAPACITY, YOU ARE EXPLICITLY AND VOLUNTARILY CONSENTING TO OUR USE, COLLECTION, ACCESS, PROCESSING, STORAGE, DISCLOSURE, TRANSFER, AND PROTECTION OF YOUR PERSONAL INFORMATION IN ACCORDANCE WITH THE TERMS SET FORTH IN THIS POLICY AND FOR THE PURPOSES DESCRIBED HEREIN. THROUGHOUT THIS DOCUMENT, ParaaCrypto IS CONSISTENTLY REFERRED TO AS EITHER ("WEBSITE" OR "PLATFORM.")

By consenting to this KYC Policy, you explicitly authorize ParaaCrypto to continuously monitor and collect information and data related to your activities on the Platform.

1. **Definition**

1.1. "**Applicable Laws**" refers to any and all statutes, laws, regulations, ordinances, rules, judgments, orders, decrees, by-laws, government approvals, resolutions, directives, guidelines, terms and conditions, or any other governmental restrictions currently in effect in India. This includes, but is not limited to, KYC and various other applicable guidelines, rules, and regulations that may be replaced, amended, or updated over time.

1.2. "**Crypto(s)" or “Cryptocurrency**” refers to digital representations of value or contractual rights that are secured through cryptography. Utilizing distributed ledger technology, these cryptocurrencies can be transferred, stored, or traded electronically via the Platform.

1.3. "**Client Due Diligence ('CDD')**" refers to the identification of a Client and/or their Beneficial Owner, alongside the verification of their identity using documents, data, or information provided by the User or obtained from reliable, independent sources. This process also encompasses Enhanced Due Diligence ('EDD') and Counterparty Due Diligence ('CPDD') as part of its comprehensive approach.

1.4. **Client**," "**User**," or "**You**" refers to any individual who uses or accesses the Platform for the purpose of trading in Cryptocurrencies.

1.5. "**Know Your Customer (‘KYC’)**" refers to a process designed to confirm and verify the identity of prospective clients and/or their beneficial owners. It serves as the principal method for identifying individuals or entities that open and operate a User Account. KYC procedures are carried out at least annually to ensure ongoing compliance and verification.

1.6. "**Officially Valid Document (OVD)**" refers to any of the following forms of identification: Passport, Driving License, proof of possession of an Aadhaar Number, Voter’s Identity Card issued by the Election Commission of India, job card issued by NREGA duly signed by a State Government officer, or a letter from the National Population Register that includes details of name and address. In this context, 'Aadhaar Number' is defined as an identification number under the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

2. KYC Standards

ParaaCrypto adheres to the Know Your Customer (KYC) standards as mandated by the Digital Personal Data Protection Act, 2023 (DPDP Act, 2023), ensuring a robust framework for authenticating the identity of our clients while safeguarding their privacy and data protection rights. ParaaCrypto systematic KYC procedures that not only verify client identities but also guarantee that the collection and processing of personal digital information are conducted with the utmost respect for individual privacy and in strict compliance with the DPDP Act.

3. Data Control

3.1. ParaaCrypto ensures that all data collection from individuals is preceded by obtaining their explicit, informed, and voluntary consent. In compliance with applicable laws, regulations, and industry best practices, ParaaCrypto has partnered with Sumsub, a global leader in compliance and identity verification solutions, to streamline and enhance the onboarding experience for its users and to perform Know Your Customer (KYC) and Know Your Business (KYB) verification processes. These procedures are essential to ensure that the Platform operates within the boundaries of legal and regulatory frameworks, particularly those pertaining to Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) standards.

3.2. ParaaCrypto provides individuals with the ongoing ability to withdraw their consent at any time. To facilitate the withdrawal of consent, ParaaCrypto offers straightforward and easily accessible channels through which individuals can communicate their decision to revoke consent. If you wish to withdraw your consent you can contact us at contact@paraacrypto.com. Upon receiving notice of revocation, ParaaCrypto will immediately cease the processing of the individual’s data, except in cases where continued processing is mandated by law. This may include situations where ParaaCrypto is required to retain data for compliance with legal

obligations or for the establishment, exercise, or defense of legal claims.

4. Data Collection from users

4.1. Identity Information: Authentication of a User is crucial for gaining access to the platform is strictly contingent upon ParaaCrypto's successful completion of the verification and Due-diligence process for each user. This stringent authentication is vital to ensure that only legitimate and verified users can engage with the service providers. Thereby enhancing scrutiny in compliance of documents. This includes names, addresses, and other demographic information essential for identifying an individual and other following are the list of documents and details that are collected from the Users:

- **4.1.1.** Full Name of the User
- **4.1.2.** Date of Birth (DOB)
- **4.1.3.** Address Proof: Utility bills, Bank Statements or other official document that confirms the current and permanent address of the User
- **4.1.4.** Photograph (Not Mandatory): Government Identification, or recent photographs may be required for verification.
- **4.1.5.** PAN card
- **4.1.6.** Aadhar Card or Passport or Voter Identity Card or any other Government Identification

4.2. **Contact Information**: Phone numbers, email addresses, and physical address details are common data points collected. This information is used for account notifications, service updates, customer support, and facilitating transactions. It also assists in resolving disputes, sending important alerts, and providing tailored service offerings based on user location or preferences

4.3. **Biometric Data**: Depending on the service, biometric data such as facial recognition data, and even voice recordings could be collected. Granted only to the verified user and reducing the risk of fraud. This type of data can also enhance user experience by streamlining the login processes and transaction verifications.

4.4. **Financial Information**: Credit card details, bank account numbers, and other financial data for processing transactions. This data is essential for executing transactions, managing subscriptions, and facilitating refunds where applicable

4.5. **Technical Information**: ParaaCrypto processes and complies with the collection of technical data including IP addresses, device identifiers like IMEI, IMSI, UUID, and MAC addresses, as well as operating system versions, device specifications, network providers, and connection details. This data helps ParaaCrypto enhance user experience, improve service security, and optimize functionality across devices and networks.

4.6. **User Data**: ParaaCrypto processes information about how users interact with the

website, including tracking URLs visited, products viewed, search history, page performance such as load times and error rates, and user engagement with the site. This data is utilized to enhance the functionality of the website, improve user experience, and optimize ParaaCrypto's products and services.

5. With whom the data will be shared

5.1. ParaaCrypto will share personal data when legally required to do so, complying with obligations under FIU and other applicable regulatory laws in India.

5.2. ParaaCrypto will share personal data when it is necessary for the performance of tasks carried out in the public interest or under the exercise of official authority vested in ParaaCrypto.

5.3. ParaaCrypto will collaborate with select third parties, such as analytics and search engine providers, to enhance and optimize our services.

6. Rights to Subject to Data

6.1. Right to Access

6.1.1. Users have the right to request access to the personal data that ParaaCrypto holds about them. This means that users can request a copy of their personal data to review the accuracy and completeness of the information collected. ParaaCrypto ensures that such requests are processed promptly and transparently, providing Users with a clear view of what data is being held and for what purpose.

6.2. Right to Correction

6.2.1. ParaaCrypto acknowledges that personal data may change over time, or inaccuracies may be identified by the data subject. In such cases, Users have the right to request corrections or updates to their personal data. ParaaCrypto facilitates these corrections, ensuring that all personal data remains accurate, up-to-date, and relevant for the purposes for which it is processed.

6.3. Right to Deletion,

6.3.1. Also known as the "right to be forgotten," this right allows Users to request the deletion or removal of their personal data when there is no compelling reason for its continued processing. ParaaCrypto respects this right and will delete personal data when requested, except in cases where ParaaCrypto is legally obligated to retain the data or if the data is necessary for compliance with a legal obligation or the defense of legal claims.

6.4. Right to Restriction of Processing

6.4.1. ParaaCrypto acknowledges the right of Users to request restrictions on the processing of their personal data. This applies particularly during the verification of data accuracy or in disputes regarding the lawfulness of

processing.

6.5. Right to Object to Processing

6.5.1. Users have the right to object to the processing of their personal data by ParaaCrypto, especially when it is based on legitimate interests or the performance of tasks carried out in the public interest or in the exercise of official authority, including profiling.

6.6. Rights Related to Automated Decision Making and Profiling

6.6.1. ParaaCrypto ensures that Users will not be subjected to decisions based solely on automated processing, including profiling, which might have legal or similarly significant effects on them.

6.7. Right to Data Portability

6.7.1. This right enables Users to receive the personal data they have provided to ParaaCrypto in a structured, commonly used, and machine-readable format. It also includes the right to transmit this data to another data controller without hindrance from ParaaCrypto. This facilitates the free movement of data across service providers, promoting competition and innovation.

6.8. Right to Withdraw Consent

6.8.1. ParaaCrypto places high importance on consent as the basis for processing personal data. Users have the right to withdraw their consent at any time. Upon receiving a notice of withdrawal, ParaaCrypto will promptly cease processing the User's data, unless another legal basis for processing exists

7. Customer Due-Diligence

7.1. ParaaCrypto employs stringent measures to verify the identity of its clients as part of the account creation process. This involves collecting reliable and official documentation that proves the identity of the customers, such as passports, driving licenses, or Aadhar card. Each document is thoroughly checked to ensure its validity and authenticity to prevent any fraudulent activities.

7.2. ParaaCrypto’s Customer Due-Diligence process involves understanding the nature of the customer’s financial activities. This helps in assessing the associated risk levels and the potential for illicit activities. By monitoring transaction patterns and comparing them against the customer’s profile, ParaaCrypto aims to identify any discrepancies or unusual activities that might suggest money laundering, terrorism financing, or other illegal activities.

7.3. ParaaCrypto is assessed for risk based on a variety of factors, including their transaction history, the types of products and services they use, and their geographic location. This risk-based approach allows ParaaCrypto to apply enhanced due diligence measures to higher-risk clients while simplifying procedures for those posing lower risks

8. Customer Identification Procedure

8.1. ParaaCrypto gathers adequate information to verify the identity of every user, regardless of whether they are regular or occasional, and to understand the purpose of the transactions being conducted on the platform.

8.2. The customer identification process involves the verification and authentication of customers by gathering and analyzing their documents and information. The specific documentation necessary for customer identification is outlined in the policy. The Company will conduct the identification process under the following circumstances:

8.2.1. Upon establishing the account-based relationship with the Customer

8.2.2. When there is doubt regarding the genuineness of the papers and information provided by the Customer

8.2.3. If there is a suspicion of money laundering and terrorist financing activities related to an existing customer of the company.

9. Data Protection

ParaaCrypto employs a multifaceted approach to data protection that emphasizes transparency, security, and client rights as follows :

9.1. ParaaCrypto implements state-of-the-art security measures to prevent unauthorized access, disclosure, alteration, or destruction of personal data. These include the use of robust encryption protocols to protect data both in transit and at rest, ensuring that all client information is securely encoded and inaccessible to unauthorized parties. Access controls are strictly enforced, with data accessibility limited to authorized personnel only, based on their role and the necessity of data access in fulfilling their duties.

9.2. Data storage is managed through secure, compliant platforms designed to prevent breaches and data loss. ParaaCrypto utilizes only those data storage solutions that meet high industry standards of security, regularly evaluating these solutions for compliance and security effectiveness.

9.3. To further ensure the integrity and security of client data, ParaaCrypto conducts regular security audits and vulnerability assessments. These assessments help identify potential security weaknesses and implement timely corrections before they can be exploited. The audits are thorough and conducted by internal teams or third-party experts to ensure unbiased scrutiny of our security practices.

9.4. In the event of a data breach or security incident, ParaaCrypto has a well-defined incident response plan that is activated immediately to mitigate the effects of the breach. This plan includes procedures for rapid response and containment, assessment of the breach’s scope and impact, notification to affected clients and regulatory authorities as required by law, and steps to prevent future occurrences.

10. Safeguarding Measures

ParaaCrypto strictly adheres to robust data security measures to safeguard personal information.

10.1. We employ data encryption to secure personal data both at rest and in transit, protecting it from unauthorized access and breaches.

10.2. Access to personal data is strictly limited to employees and third parties who require it to perform their duties, supported by rigorous authentication and authorization practices.

10.3. We conduct regular audits to identify and address potential vulnerabilities or compliance gaps and practice data minimization by collecting only the necessary data for explicitly stated purposes, ensuring it is not retained longer than needed.

10.4. We provide ongoing security training to all employees to enhance their awareness of data protection responsibilities.

10.5. ParaaCrypto maintains an effective incident response plan to swiftly manage and mitigate the impacts of data breaches, ensuring compliance with legal obligations and clear communication with stakeholders.

10.6. Our vendor management ensures that all third-party service providers comply with the DPDP Act through strict data security and processing agreements.

10.7. We incorporate privacy by design principles into the development and operation of IT systems and maintain the integrity and confidentiality of personal data at all times.

11. Consent

By using this platform , you acknowledge, understand, and agree to comply with the terms set forth in this KYC Policy. If you do not agree with the terms of this KYC Policy, please refrain from using the Platform.

ParaaCrypto values your trust and is committed to ensuring a secure user experience while prioritizing your safety. We aim to provide a satisfactory experience on the Platform and assure you that your data is treated with the utmost importance.

If you have any questions or concerns about our KYC Policy or any other aspect of the Platform, please do not hesitate to reach out to us using the contact information provided. We are dedicated to addressing your inquiries promptly and maintaining transparency regarding our data handling practices.