Anti-Money Laundering Policy (AML) for Paraacrypto Exchange Wallet

I. Overview

This Anti-Money Laundering (AML) Policy has been meticulously designed to ensure compliance with all applicable laws, rules, and regulations, including but not limited to the Prevention of Money Laundering Act, 2002 (PMLA), its associated rules, and global standards such as the recommendations of the Financial Action Task Force (FATF). By establishing a comprehensive and actionable framework, ParaaCrypto Exchange Wallet ("ParaaCrypto" or "the Company") demonstrates its commitment to identifying, preventing, and mitigating risks associated with money laundering, terrorist financing, and other financial crimes. This policy is integral to the Company's mission of fostering a secure, transparent, and trustworthy cryptocurrency trading environment.

Commitment to Compliance and Integrity: ParaaCrypto integrates advanced systems, controls, and procedural safeguards to achieve and maintain full compliance with Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) standards, in alignment with both Indian regulatory frameworks and global best practices. Leveraging state-of-the-art technologies, such as real-time transaction monitoring, fraud detection algorithms, and enhanced data analytics, the Company proactively safeguards its platform against misuse by illicit actors. ParaaCrypto's commitment extends beyond compliance, actively contributing to global efforts aimed at combating financial crimes and ensuring the integrity of financial ecosystems worldwide.

Roles and Responsibilities: This AML Policy clearly delineates the roles and responsibilities of all stakeholders, including ParaaCrypto, its employees, users, agents, and third-party service providers. The implementation of robust Know Your Customer (KYC) and Customer Due Diligence (CDD) measures are central to the Company's strategy, ensuring accurate identification of users and their activities. Through a proactive culture of compliance, ParaaCrypto not only fulfills its legal obligations but also enhances user trust, regulatory confidence, and platform integrity. Employees and stakeholders are continually empowered through rigorous training programs, clear operational guidelines, and periodic awareness initiatives to remain vigilant and informed about emerging risks and regulatory changes.

II. Objectives

1. **Prevention of Financial Crimes :** At the forefront of its objectives, ParaaCrypto is dedicated to prevent its platform from being exploited for illicit activities such as money laundering, terrorist financing, and other financial crimes. Through diligent monitoring and strict adherence to regulatory requirements, the Company ensures the maintenance of a secure and transparent trading ecosystem that protects the interests of all stakeholders.
2. **Establishment of Robust Systems:** The Company employs advanced technologies, including multi-signature protocols, automated transaction monitoring systems, and AI-driven fraud detection mechanisms. These systems are designed to not only meet but exceed regulatory requirements, ensuring a proactive and effective approach but also to avert risk management and the identification of suspicious activities.

3. **Regulatory Compliance:** ParaaCrypto adheres to all relevant AML regulations, including the provisions of the Prevention of Money Laundering Act, 2002 (PMLA), and aligns with international standards such as FATF recommendations. By implementing globally recognized best practices, the Company ensures consistent compliance with evolving legal and regulatory landscapes across all jurisdictions where it operates.
4. **Support for Law Enforcement:** ParaaCrypto actively collaborates with law enforcement agencies, regulatory bodies, and other competent authorities to support the detection, investigation, and prosecution of financial crimes. This includes the timely reporting of suspicious transactions, the maintenance of detailed and accurate records, and the provision of necessary information to aid investigations.
5. **Culture of Compliance:** Recognizing that effective AML compliance is a collective effort, ParaaCrypto fosters a culture of accountability and integrity within its organization. Through ongoing training, regular communication, and dedicated resources, the Company ensures that all employees and stakeholders are well-informed about their responsibilities under the AML framework. This culture of compliance not only mitigates risks but also reinforces the trust and confidence of users, regulators, and partners.

III. Scope

This Anti-Money Laundering (AML) Policy applies comprehensively to all stakeholders involved with ParaaCrypto Exchange Wallet ("ParaaCrypto" or "the Company"), ensuring a unified and consistent approach to combating financial crimes. The scope encompasses:

1. **Users:** All individual and institutional users of the platform are required to adhere to stringent KYC (Know Your Customer) and AML protocols. Users must provide accurate and verifiable information, comply with transaction monitoring requirements, and cooperate with any additional documentation requests during due diligence processes. Non-compliance may result in account restrictions or suspension.
2. **Employees:** ParaaCrypto's employees are integral to the effective implementation of its AML Policy. They are responsible for strictly following internal AML procedures, promptly reporting any suspicious activities, and participating in regular training programs designed to enhance awareness of AML risks, evolving threats, and regulatory changes.
3. **Agents and Third-Party Providers:** Consultants, agents, and service providers, such as those managing KYC processes or transaction monitoring systems, are required to operate in full alignment with ParaaCrypto's AML standards. Third-party providers must sign formal acknowledgments affirming their commitment to compliance, conduct regular audits, and implement industry-leading practices for data security and customer due diligence.
4. **Global Applicability:** Given its international operations, ParaaCrypto is committed to maintaining compliance with AML laws across all jurisdictions where it operates. Where discrepancies exist between local and global regulations, the Company applies the stricter standard to uphold its integrity and commitment to combating financial crimes.

IV. KYC and Customer Due Diligence (CDD)

1. **Verification of Identity and Address:** ParaaCrypto employs robust KYC protocols to establish and verify the identity of its customers. Through a strategic partnership with Sumsub, a secure identity verification platform, the Company uses advanced AI-based technologies to ensure accuracy and efficiency. The verification process involves:

- **Government-issued IDs**: Including passports, driver's licenses, and national ID cards.
- **Address Verification**: Utilizing utility bills, bank statements, or other acceptable documentation.
- This rigorous approach helps prevent the creation of fictitious, anonymous, or benami accounts, ensuring compliance with global standards.

2. **Assessment of Customer Activities:** Customers are required to disclose the intended purpose of their transactions and provide details about the sources of their funds. ParaaCrypto leverages external databases and advanced analytics to validate the legitimacy of this information and to identify potential red flags that may indicate suspicious or high-risk activities.

3. **Risk-Based Classification:** ParaaCrypto uses a risk-based approach to classify customers into **low**, **medium**, and **high-risk** categories. This classification is based on factors such as:

- Transaction patterns and frequency.
- Geographic location and regulatory risks.
- Type of account and activities conducted.

4. **High-risk customers**: including those with unusual transaction behavior or those from high-risk jurisdictions, undergo Enhanced Due Diligence (EDD). EDD involves:

- Additional documentation requirements.
- Senior management approval for specific high-risk activities.
- More frequent and detailed reviews of transactions.

5. **Special Categories of Customers (CSC):** Certain categories of customers are subject to stricter measures to address inherent risks. These include:

- **Politically Exposed Persons (PEPs)**: Individuals holding prominent public positions and their family members or associates.
- **High-Net-Worth Individual**

6. **Ongoing Monitoring and Updates:** ParaaCrypto maintains continuous monitoring systems to detect unusual or suspicious activities in real-time. These systems include automated alerts for anomalies such as:

- Large or unusual transactions inconsistent with the customer's profile.
- High-frequency transactions without clear economic rationale.
- Transactions linked to high-risk jurisdictions or flagged accounts.
- Customer risk profiles are reassessed periodically to reflect changes in behavior, account activities, or external risk indicators. Alerts for suspicious transactions are promptly escalated to the compliance team for thorough investigation and, where necessary, reported to regulatory authorities.

7. **Record Retention and Data Security:** To ensure compliance with regulatory requirements, ParaaCrypto retains all customer records, including KYC documents and transaction histories, for the legally mandated period. These records are protected using advanced encryption technologies to prevent unauthorized access, breaches, or data leaks. Confidentiality is paramount, and disclosures are made only under legal mandates or at the request of competent regulatory authorities.

V. **Prohibited Activities**

ParaaCrypto Exchange Wallet ("ParaaCrypto" or the "Company") enforces strict prohibitions on activities that violate its AML Policy, applicable regulations, or international standards. These measures ensure the platform's integrity, compliance, and protection against illicit use. The following activities are explicitly prohibited:

1. Opening Accounts in Fictitious, Benami, or Anonymous Names

- The creation or maintenance of accounts under false identities, aliases, or fictitious names is strictly forbidden.
- Benami accounts, where ownership is concealed by registering accounts in another person's name, are prohibited.
- To prevent anonymity, ParaaCrypto mandates comprehensive **KYC verification**, ensuring all accounts are linked to legitimate, identifiable individuals or entities.

2. Non-Compliant or Evasive Transactions

Transactions that circumvent regulations or evade detection mechanisms are strictly disallowed, including but not limited to:

- **Structuring (Smurfing):** Dividing large transactions into smaller amounts to bypass reporting thresholds.
- **Layering:** Engaging in multiple, complex transactions to obscure the source of funds.
- **Circular Transactions:** Repeatedly moving funds across accounts without a clear economic purpose.
- Any suspicious transaction identified through ParaaCrypto's advanced monitoring system will be immediately escalated for investigation and reported to the appropriate regulatory authorities.

3. Facilitating Transactions Involving Banned or Sanctioned Individuals or Entities

- Transactions involving individuals, entities, or organizations restricted by local or international regulatory authorities are prohibited.
- ParaaCrypto regularly screens accounts and transactions against global sanction lists, including but not limited to:
    - **United Nations Security Council (UNSC) Sanctions List.**
    - **Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) List.**

    - **European Union Sanctions List and other jurisdiction-specific lists.**
- Accounts linked to sanctioned entities or individuals will be immediately frozen, with related transactions reported to the relevant authorities as per regulatory requirements.

4. <u>Transactions Involving High-Risk Jurisdictions or Activities</u>

ParaaCrypto applies enhanced due diligence to transactions linked to high-risk jurisdictions or activities. It prohibits transactions associated with:

- Jurisdictions flagged as high-risk by **FATF** or other international organizations.
- Activities such as:
    - **Human trafficking or exploitation.**
    - **Arms trafficking or proliferation of weapons of mass destruction (WMD).**
    - **Narcotics trafficking or illicit drug-related activities.**

5. **<u>Use of the Platform for Fraudulent or Illegal Activities:</u>**

Paraacrypto Exchange Wallet ("Paraacrypto") is steadfast in its commitment to ensuring that its platform is not exploited for any fraudulent or illegal activities. The misuse of the platform for such purposes undermines its integrity, exposes the Company to regulatory risks, and compromises its compliance with applicable anti-money laundering (AML) and counter-terrorism financing (CTF) laws. Consequently, Paraacrypto has implemented strict policies and controls to detect, prevent, and address any instances of fraudulent or illicit activities. The following elaborates the Company's stance and measures concerning the use of its platform.

A. **<u>Prohibition of Fraudulent Activities:</u>** Paraacrypto categorically prohibits the use of its platform for activities that involve fraud, deception, or misrepresentation. Fraudulent activities may include but are not limited to:

- The creation or use of fake or unauthorized accounts to conduct transactions.
- Misrepresentation of identity, financial status, or the purpose of transactions to gain access to the platform or to engage in suspicious financial activities.
- The manipulation of transaction records, account balances, or other data to deceive the platform, customers, or third-party partners.

Any attempts to engage in such activities will not only result in immediate account suspension or termination but may also be reported to the relevant law enforcement authorities for further investigation and potential prosecution.

B. **<u>Prohibition of Tax Evasion:</u>** Paraacrypto strictly forbids the use of its services to evade tax obligations. Tax evasion, which involves the deliberate misrepresentation of financial information to reduce or avoid tax liabilities, is a criminal offense in most jurisdictions. The platform actively monitors transactions to identify and flag patterns that may indicate attempts to conceal taxable income, transfer funds to evade taxes, or engage in any activities designed to subvert tax laws.

Customers using Paraacrypto's services are reminded that they are fully responsible for complying with the tax regulations applicable in their jurisdiction and for accurately reporting their income and transactions as required by law.

C. **Prevention of Other Illegal Activities:** The platform is equally vigilant against being used for other illegal purposes, including but not limited to:

- Facilitating the financing of criminal enterprises or organized crime.
- Participating in the trade of illicit goods or services, such as drugs, weapons, or counterfeit products.
- Supporting activities related to human trafficking, child exploitation, or other egregious violations of human rights.

Paraacrypto has deployed advanced monitoring systems that analyze transaction data for signs of unusual or suspicious behavior indicative of such illegal activities. Any such incidents detected are subject to immediate action, including the suspension of services and reporting to the relevant authorities as required under applicable AML/CTF laws.

D. **Prohibition of Bypassing AML Measures:** Attempts to bypass or circumvent Paraacrypto's AML and compliance measures are expressly prohibited. Such attempts include but are not limited to:

- Providing false or misleading information during the Know Your Customer (KYC) and Customer Due Diligence (CDD) processes.
- Submitting forged, altered, or otherwise fraudulent documents to gain unauthorized access to the platform.
- Engaging in activities designed to obscure the origin, purpose, or destination of funds, such as structuring transactions to avoid reporting thresholds or using third-party intermediaries to disguise financial flows.

Paraacrypto employs stringent identity verification procedures, real-time transaction monitoring, and robust data validation systems to identify and block such attempts. Customers found to have engaged in these practices will face severe consequences, including the permanent closure of their accounts, forfeiture of funds where applicable, and legal action under the relevant laws and regulations.

E. **Legal and Regulatory Consequences**: Paraacrypto underscores that any involvement in fraudulent or illegal activities is not only a violation of the platform's terms of service but also a breach of applicable legal and regulatory frameworks. Customers who engage in such activities may face significant penalties, including fines, imprisonment, and asset forfeiture, as stipulated under local and international laws. Additionally, Paraacrypto reserves the right to cooperate fully with law enforcement and regulatory authorities by providing information and evidence necessary for the investigation and prosecution of such offenses.

VI. Reporting Suspicious Transactions:

Paraacrypto Exchange Wallet ("Paraacrypto") is committed to fulfilling its obligations under the Prevention of Money Laundering Act, 2002 ("PMLA") and other applicable regulations by establishing a robust mechanism for detecting, reporting, and addressing suspicious transactions. Reporting suspicious activities is a critical component of Paraacrypto's Anti-Money Laundering (AML) framework, aimed at preventing the platform from being misused for illicit purposes, including money laundering, terrorist financing, or other financial crimes.

A. **Responsibilities of Employees and Agents:** All employees and agents of Paraacrypto, including those engaged through third-party service providers, are required to remain vigilant and report any transaction that appears suspicious or inconsistent with a customer's known profile or transactional behavior. Suspicious transactions may include, but are not limited to:

- Transactions that lack an apparent economic rationale or legitimate purpose.
- Transfers involving unusually large sums of money, particularly if they do not align with the customer's stated financial activities.
- Transactions with complex structures designed to obscure the origin or destination of funds.
- Transactions originating from or directed to high-risk jurisdictions or individuals/entities on sanction lists.
- Employees and agents must report these transactions immediately to the designated Principal Officer. Under no circumstances should they disclose the suspicion to the customer or any unauthorized party, as doing so could compromise ongoing investigations or regulatory processes.

B. **Role of the Principal Officer:** The Principal Officer is the designated individual responsible for overseeing Paraacrypto's AML compliance program, including the reporting of suspicious transactions. Upon receiving a report of suspicious activity, the Principal Officer shall:

- Review the Report: Conduct a detailed review of the transaction(s) flagged as suspicious to verify the validity of the concerns raised. This review may involve examining customer records, transaction history, and any other relevant documentation.
- Determine the Next Steps: Based on the review, the Principal Officer shall decide whether the transaction warrants further scrutiny or reporting to external authorities.
- Prepare and Submit Reports: If the transaction meets the criteria for a Suspicious Transaction Report (STR) under the PMLA, the Principal Officer shall prepare and **submit the report to the Financial Intelligence Unit-India (FIU-IND)** in the prescribed format and within the required timeframe.

C. **Definition of Suspicious Transactions:** A suspicious transaction is any activity that deviates from a customer's usual financial behavior, raises concerns about the source or purpose of funds, or appears to contravene applicable laws and regulations. Examples include:

- Unusual Volume or Frequency: Repeated transactions involving unusually large amounts or frequent transfers inconsistent with the customer's normal activity.

- Disguised Identity: Transactions where the customer's identity is unclear, documents appear fraudulent, or the customer refuses to provide requested information.
- Layering Techniques: Activities designed to obscure the origin of funds, such as splitting large transactions into smaller amounts or routing funds through multiple intermediaries.
- High-Risk Profiles: Transactions involving politically exposed persons (PEPs), customers from high-risk jurisdictions, or individuals/entities listed on international sanctions or watchlists.

D. **Reporting Obligations to FIU-IND**: As mandated under the PMLA, Paraacrypto shall report suspicious transactions to the Financial Intelligence Unit-India (FIU-IND) promptly and in the prescribed format. The Principal Officer will ensure that:

- All necessary details of the transaction, including customer information, transaction amount, date, and nature of the activity, are accurately documented in the STR.
- The STR is submitted within the specified deadline to avoid non-compliance penalties.
- Additional information or clarification requested by FIU-IND is provided in a timely manner to facilitate further investigation.

E. **Confidentiality and Protection of Whistleblowers:** To encourage employees and agents to report suspicious transactions without fear of retaliation, Paraacrypto ensures strict confidentiality of all reports made. The identity of the reporting individual shall not be disclosed to unauthorized persons or entities. Additionally, Paraacrypto has instituted safeguards to protect whistleblowers from any adverse consequences resulting from their actions taken in good faith.

VII. Record Maintenance and Retention:

Paraacrypto Exchange Wallet ("Paraacrypto") is committed to maintaining comprehensive and accurate records of all customer interactions, transactions, and related documentation to comply with applicable regulations and facilitate effective monitoring, investigation, and reporting of suspicious activities. Proper record maintenance and retention are fundamental to Paraacrypto's Anti-Money Laundering (AML) program, as they ensure transparency, traceability, and accountability in financial transactions conducted on the platform.

A. **General Record Retention Policy:** In compliance with the Prevention of Money Laundering Act, 2002 ("PMLA"), and global best practices, Paraacrypto shall maintain records of all transactions and customer information for a minimum of ten (10) years. This retention period shall be calculated from the later of the following dates:

- The date of cessation of the customer relationship.
- The date of the transaction in question.

The records to be maintained include, but are not limited to:

- Identity Documents: Copies of all documents used for Know Your Customer (KYC) verification, including government-issued identification, proof of address, and other relevant credentials.

- Transaction Details: Comprehensive records of transactions conducted on the platform, including transaction amounts, dates, account details, and counterparties involved.
- Risk Assessment and Monitoring Records: Documentation of customer risk profiles, due diligence procedures, and monitoring activities.
- Communications: Records of any communications with customers related to transactions, account activities, or compliance matters.

B. **Retention of Suspicious Transaction Records:** For transactions flagged as suspicious, Paraacrypto shall retain all related records and documentation until the investigation is fully resolved and confirmation is received from the relevant authorities that no further action is required. These records shall include:

- Detailed Suspicious Transaction Reports (STRs) submitted to the Financial Intelligence Unit-India (FIU-IND).
- Correspondence with FIU-IND and other regulatory or law enforcement agencies.
- Any additional information obtained during the investigation, such as customer explanations or responses.

C. **Accessibility of Records:** Paraacrypto ensures that all records are stored in a secure but readily accessible manner to facilitate:

- Internal audits and reviews of AML compliance.
- Prompt responses to requests from regulatory or law enforcement authorities.
- Support for legal proceedings, investigations, or risk assessments.

D. **Security and Confidentiality of Records:** To protect the integrity and confidentiality of customer data, Paraacrypto employs robust data security measures, including:

- Encryption and secure storage of electronic records.
- Restricted access to sensitive records, with access granted only to authorized personnel.
- Regular audits of record-keeping systems to identify and mitigate any potential vulnerabilities.

E. **Destruction of Records:** Upon the expiration of the retention period, records no longer required for regulatory or legal purposes shall be securely destroyed in compliance with data protection laws and internal policies. This may involve:

- Permanent deletion of electronic records using secure data erasure methods.
- Shredding or incineration of physical records under controlled conditions.

VIII. Monitoring and Internal Controls

ParaaCrypto Exchange Wallet ("ParaaCrypto" or "the Company") is dedicated to maintaining a robust system of monitoring and internal controls to comply with Anti-Money Laundering (AML) laws and

regulations, including the **Prevention of Money Laundering Act, 2002 (PMLA)**, and guidelines from relevant regulatory authorities. These measures aim to prevent, detect, and address risks associated with money laundering, terrorist financing, and other financial crimes, ensuring the integrity and security of the platform.

1. Transaction Monitoring Systems

ParaaCrypto employs advanced transaction monitoring systems to proactively identify and address suspicious activities. Key features of the monitoring framework include:

- **Automated Detection Mechanisms:** Utilizing predefined risk parameters to flag transactions that:
    - Exceed typical thresholds (e.g., unusually large sums).
    - Occur with high frequency or deviate from the customer's risk classification and declared profile.
    - Exhibit patterns indicative of structuring (smurfing), layering, or circular transactions designed to obscure the origin of funds.
- **Real-Time Alerts:** Immediate generation of alerts for flagged transactions, which undergo detailed investigation by the compliance team.
- **Advanced Analytics:** Leveraging machine learning and AI to detect trends, patterns, and anomalies indicative of financial crimes.
- **Escalation and Reporting:** Transactions deemed suspicious are escalated to the compliance team for in-depth scrutiny. When required, reports are submitted to the **Financial Intelligence Unit-India (FIU-IND)** or other relevant authorities in accordance with regulatory obligations.

2. Regular Audits and Reviews

To ensure the ongoing effectiveness of its AML framework, ParaaCrypto conducts periodic audits and reviews of its internal controls, systems, and procedures. These audits aim to:

- Evaluate the adequacy of existing monitoring mechanisms and their ability to identify and report suspicious activities.
- Identify gaps, vulnerabilities, or inefficiencies in the AML program and recommend improvements.
- Ensure compliance by employees, agents, and third-party service providers with the Company's AML policies.
- Verify that all flagged transactions are appropriately documented and reported to the relevant authorities.

Audits are performed by:

- **Internal Compliance Teams:** Conducting routine reviews to maintain system integrity.
- **External Audit Firms:** Providing independent assessments and expertise in AML compliance.

Findings from these audits are presented to senior management, along with actionable recommendations for addressing identified deficiencies.

3. Roles and Responsibilities

- **Principal Officer:** The Principal Officer oversees the implementation and management of monitoring systems, ensuring sufficient resources and operational efficiency.
- **Compliance Team:** Investigates flagged transactions, enforces AML protocols, and liaises with regulatory bodies.
- **Employees and Agents:** All staff and representatives are required to report anomalies promptly and cooperate fully with the monitoring process.

4. Confidentiality and Safeguards

Recognizing the sensitive nature of transaction monitoring and reporting, ParaaCrypto enforces strict confidentiality protocols to protect customer data and operational integrity:

- Access to flagged transaction details and customer profiles is restricted to authorized personnel.
- Data encryption and secure storage mechanisms safeguard sensitive information.
- Information disclosure is strictly limited to regulatory authorities or as required by law.

5. Legal Consequences of Non-Compliance

Failure to maintain effective monitoring systems and internal controls may result in:

- Significant legal penalties and sanctions.
- Reputational harm that undermines user trust and business credibility.
- Regulatory interventions affecting platform operations.

To mitigate these risks, ParaaCrypto commits to:

- **Continuous Improvement:** Regular updates to its monitoring systems and internal controls to address evolving threats and regulatory requirements.
- **Employee Training:** Providing ongoing AML education to ensure awareness of compliance obligations and best practices.

IX. **Employee Training and Confidential Reporting:**

Paraacrypto Exchange Wallet ("Paraacrypto" or "the Company") recognizes that the success of its Anti-Money Laundering (AML) program depends heavily on the awareness and active participation of its employees. To ensure compliance with applicable AML regulations, including the Prevention of Money Laundering Act, 2002 ("PMLA"), and associated guidelines, the Company is committed to equipping its employees with the knowledge and tools necessary to identify and mitigate risks related to money laundering, terrorist financing, and other financial crimes. Furthermore, the Company shall maintain a framework for the confidential reporting of any instances of non-compliance or violations of this policy, thereby fostering a culture of transparency and accountability.

A. **Ongoing Employee Training Programs:** Paraacrypto shall organize and conduct regular training programs tailored to the roles and responsibilities of its employees, agents, and other stakeholders involved in the implementation of the AML framework. These training programs shall aim to:

- Educate employees on the significance of AML regulations and their critical role in ensuring the Company's compliance with legal and regulatory requirements.
- Provide detailed guidance on identifying red flags and suspicious activities, including but not limited to unusual transaction patterns, attempts to evade customer due diligence, and transactions involving high-risk customers or jurisdictions.
- Familiarize employees with the Company's internal policies, procedures, and systems for detecting, monitoring, and reporting suspicious transactions.
- Ensure that employees are aware of their reporting obligations and the processes for escalating concerns or anomalies to the appropriate authorities within the organization.
- Keep employees updated on changes in AML regulations, emerging risks, and global best practices.
- Training sessions shall be conducted upon onboarding new employees and at regular intervals throughout their employment. Participation in these programs shall be mandatory, and attendance records shall be maintained for audit and compliance purposes.

B. **Confidential Reporting Mechanism:** To safeguard the integrity of its AML framework, Paraacrypto shall establish a confidential reporting mechanism that enables employees to report any instances of non-compliance, policy violations, or suspicious activities without fear of retaliation or adverse consequences. The following measures shall be implemented:

- Reporting to the Principal Officer or Managing Director: Employees may report concerns directly to the designated Principal Officer or the Managing Director, who shall ensure that all reports are treated with utmost confidentiality and investigated thoroughly.
- Anonymity and Protection: Employees shall have the option to report anonymously, and the Company shall take all necessary steps to protect the identity of whistleblowers and shield them from any form of harassment, discrimination, or reprisal.
- Investigation and Resolution: The Principal Officer, in collaboration with other relevant stakeholders, shall investigate all reported incidents promptly and take appropriate corrective or disciplinary action as warranted.
- Record-Keeping and Reporting: All reports of non-compliance or violations shall be documented, and significant cases shall be escalated to senior management or regulatory authorities as required by law.

C. **Accountability and Non-Tolerance for Non-Compliance:** Paraacrypto shall adopt a zero-tolerance approach toward non-compliance with its AML policy, internal procedures, or applicable regulations. Employees found to be complicit in violations or failing to fulfill their AML obligations may face disciplinary action, up to and including termination of employment, in addition to any legal consequences prescribed under applicable laws.

X. **Amendment and Review:**

This Anti-Money Laundering (AML) Policy shall remain a dynamic document, subject to periodic review and updates to ensure its continued relevance, effectiveness, and compliance with applicable laws, regulations, and guidelines. Paraacrypto Exchange Wallet ("Paraacrypto" or "the Company") recognizes the importance of adapting to evolving legal and regulatory frameworks and emerging risks in the global financial landscape. The Company shall undertake a thorough review of this policy at regular intervals or whenever significant changes occur in AML-related statutes, rules, or guidelines issued by regulatory

authorities. The review process shall include an assessment of the policy's adequacy in addressing risks associated with money laundering, terrorist financing, and other illicit financial activities. Any deficiencies identified during the review shall be rectified through amendments to the policy, ensuring that it remains robust and effective.

A. **Incorporation of Statutory Amendments:** Any amendments to applicable statutory provisions, including but not limited to the Prevention of Money Laundering Act, 2002 (PMLA), and associated regulations or directives issued by competent authorities, shall be deemed automatically incorporated into this policy. Such statutory changes shall take immediate effect and shall be reflected in the Company's operational procedures and systems. The updated policy shall then be formally presented to the Company's Board of Directors for review and approval.

B. **Board Approval and Oversight:** The Board of Directors shall maintain ultimate responsibility for the oversight and approval of this policy, including any proposed amendments. All modifications to the policy, whether resulting from changes in statutory requirements, operational needs, or audit findings, shall be submitted to the Board for review. The Board shall ensure that any amendments align with the Company's commitment to compliance and risk management.

C. **Employee Notification and Training:** Following any amendments, Paraacrypto shall notify all employees, agents, and relevant stakeholders of the changes to the policy. Training programs shall be updated accordingly to familiarize employees with new provisions and ensure their effective implementation.

D. **Audit and Reporting:** Periodic audits shall be conducted to assess the implementation and effectiveness of the amended policy. Any findings or recommendations resulting from these audits shall be reviewed by senior management, and corrective measures shall be implemented promptly. The Principal Officer shall also ensure that any material changes to the policy are reported to regulatory authorities as required.

XI. Communication:

The effective implementation of this Anti-Money Laundering (AML) Policy hinges on clear, consistent, and transparent communication to all relevant stakeholders. Paraacrypto Exchange Wallet ("Paraacrypto" or "the Company") recognizes the necessity of disseminating the policy's provisions, obligations, and expectations to ensure compliance and alignment across all levels of its operations.

A. **Role of the Principal Officer:** The Principal Officer, as the designated compliance authority within the Company, shall bear the primary responsibility for ensuring that this AML Policy is effectively communicated to all relevant stakeholders. This includes employees, third-party service providers, agents, and customers. The Principal Officer shall employ structured and systematic methods to ensure that all parties understand their roles and responsibilities as outlined in this policy.

B. **Communication with Employees:** Employees, being the frontline actors in the implementation of this policy, shall receive comprehensive training and written guidelines detailing their obligations

under the AML framework. The Principal Officer shall ensure that the policy is made accessible to all employees via internal communication channels, including employee handbooks, intranet portals, and dedicated training sessions. Periodic updates to the policy shall also be promptly communicated, ensuring that employees remain informed about any changes or amendments.

C. **Engagement with Third-Party Service Providers**: Third-party service providers engaged by Paraacrypto for KYC, customer due diligence, and other AML-related functions must be fully apprised of the provisions of this policy. The Principal Officer shall ensure that these service providers receive copies of the policy and are contractually obligated to adhere to its requirements. Any lapses in compliance by third-party entities shall be treated as a violation of this policy and addressed accordingly.

D. **Customer Awareness:** To foster transparency and trust, Paraacrypto shall ensure that its customers are aware of the Company's AML measures. Relevant portions of this policy, including those pertaining to KYC requirements, customer due diligence, and prohibited activities, shall be communicated to customers through publicly accessible channels such as the Company's website, terms of service, and user agreements. Customers shall also be notified of their responsibilities, including the obligation to provide accurate and complete information during the onboarding process.

E. **Feedback and Queries:** The Principal Officer shall establish mechanisms for stakeholders to seek clarification on the provisions of this policy and provide feedback. Employees, third-party service providers, and customers shall have access to designated channels for addressing their concerns or reporting any potential violations of this policy.

F. **Periodic Review of Communication Practices:** The effectiveness of communication efforts shall be assessed periodically to ensure that all stakeholders remain informed and aligned with the Company's AML objectives. The Principal Officer shall oversee this review process and recommend improvements to enhance clarity, accessibility, and outreach.

XII. Acknowledgment by Third-Party KYC Service Providers

To ensure the seamless implementation of its Anti-Money Laundering (AML) Policy, **ParaaCrypto Exchange Wallet ("ParaaCrypto" or "the Company")** mandates that all third-party service providers engaged for Know Your Customer (KYC) compliance formally acknowledge and commit to adhering to the provisions of this policy. This acknowledgment is essential for maintaining the integrity of ParaaCrypto's operations and ensuring compliance with all applicable AML laws, including the **Prevention of Money Laundering Act, 2002 (PMLA)**, and related regulations.

A. **Formal Acknowledgment and Commitment:**

Before engagement, third-party service providers must submit a written acknowledgment affirming their compliance with:

1. **Regulatory Requirements:** Full adherence to the provisions of this policy and all relevant AML laws and guidelines.

2. **Policy Standards:** Implementation of robust KYC and Customer Due Diligence (CDD) processes as outlined by ParaaCrypto.

B. Key Obligations for Third-Party KYC Service Providers

1. **Implementation of Robust KYC Measures:**
    - Conduct identity verification, risk categorization, and due diligence processes that meet or exceed regulatory standards and global best practices.
    - Ensure that no accounts are opened for individuals or entities without proper verification and validation.
2. **Compliance with Risk-Based Procedures:**
    - Apply a risk-based approach to customer classification and monitoring, in alignment with ParaaCrypto's AML Policy.
    - Implement enhanced due diligence (EDD) for high-risk customers or transactions, as required.
3. **Data Security and Confidentiality:**
    - Protect all customer information using advanced encryption and secure storage protocols to prevent unauthorized access or breaches.
    - Maintain strict confidentiality and disclose customer data only as required by law or with explicit authorization from ParaaCrypto.
4. **Reporting and Cooperation:**
    - Promptly report any suspicious activities identified during the KYC process to ParaaCrypto's designated **Principal Officer** or compliance team.
    - Cooperate fully with any audits, investigations, or reviews conducted by the Company or regulatory authorities.
5. **Periodic Reviews and Updates:**
    - Regularly evaluate and update internal procedures to align with evolving regulatory requirements and amendments to ParaaCrypto's AML Policy.
    - Ensure timely communication with ParaaCrypto regarding any changes in procedures, tools, or technologies used for compliance purposes.

C. Consequences of Non-Compliance

Failure to comply with the requirements outlined in this policy or any instance of non-compliance may result in:

- **Immediate Termination of Engagement:** The business relationship will be terminated with immediate effect.
- **Regulatory Reporting:** Instances of non-compliance will be reported to the relevant authorities, as deemed necessary.

D. Strategic Importance of Third-Party Compliance

This acknowledgment serves as a cornerstone of ParaaCrypto's AML framework, ensuring that all third-party KYC service providers align with the Company's commitment to combating money laundering and

terrorist financing. Through these collaborative efforts, ParaaCrypto reinforces its dedication to maintaining a secure, transparent, and compliant platform.

XIII. **Confidentiality:**

Paraacrypto Exchange Wallet is committed to maintaining the confidentiality of all reports and communications related to suspicious transactions, in strict compliance with applicable laws. This principle of confidentiality applies to the Company, its employees, agents, and any third-party service providers engaged in the performance of AML-related functions. As per legal requirements, including the provisions of the PMLA, employees, agents, and third parties are strictly prohibited from disclosing, directly or indirectly, to any customer or third party that a suspicious transaction report (STR) has been or will be filed with the Financial Intelligence Unit-India (FIU-IND) or any other regulatory authority. Any such disclosure, whether intentional or unintentional, constitutes a violation of the law and this policy, and may lead to disciplinary action, termination of engagement, and potential legal consequences. To uphold this obligation, Paraacrypto shall implement the following measures:

- **Restricted Access to STR Information**: Access to information about suspicious transactions shall be strictly limited to authorized personnel, including the Principal Officer and designated compliance officers.
- **Training and Awareness:** Employees and agents shall be trained on their confidentiality obligations, emphasizing the importance of non-disclosure and the legal ramifications of a breach.
- **Secure Communication Channels:** All reports and communications related to suspicious transactions shall be transmitted using secure and confidential channels to prevent unauthorized access or disclosure.
- **Monitoring and Enforcement:** The Company shall monitor compliance with confidentiality obligations and take immediate action against any individual or entity found to be in violation.

This agreement is binding upon Paraacrypto and its users, employees, and third-party service providers.