KYC / AML POLICY FOR CUSTOMER IDENTIFICATION, PREVENTION OF MONEY LAUNDERING, AND TRANSACTION MONITORING

This policy outlines the KYC and AML requirements for using the SunCrypto website (https://suncrypto.in/) and mobile application called "SunCrypto: Cryptocurrency App" (collectively referred to as the "Platform"). The Platform is owned and managed by Angelic Infotech Private Limited, a company incorporated under the Companies Act, 2013, operating under the brand name of "SunCrypto".

By accessing the Platform, you acknowledge that this KYC/AML Policy is a binding agreement between you and SunCrypto. SunCrypto reserves the right to modify, add or remove parts of this policy at any time without prior notice. It is your responsibility to review this policy periodically for updates. Your use of the Platform after any modifications will indicate your acceptance of the changes. This KYC/AML Policy is also subject to the Terms of Use and Privacy Policy of the Platform.

By accessing the Platform, you agree to allow SunCrypto to continuously monitor and collect data and information about your activities on the Platform for the purpose of this KYC/AML Policy.

MEANING OF TERMS USED IN THIS POLICY:

- The term "Applicable Law" refers to any existing and enforceable legal regulations, such as statutes, ordinances, rules, judgments, orders, decrees, guidelines, policies, directives, requirements, or other governmental restrictions in India. This includes the Prevention of Money Laundering Act 2002 ("PMLA"), the Prevention of Money Laundering (Maintenance of Records) Rules 2005 ("PML Rules"), as well as various applicable regulations, rules, and guidelines of the Reserve Bank of India, its constituents/payment system providers, and the Computer Emergency Response Team, India, which may be updated or replaced from time to time.
- The term "Crypto(s)" denotes virtual digital assets that are cryptographically secured and represented as a digital value or contractual right, using distributed ledger technology. These can be traded, stored, or transferred electronically using the Platform, including bitcoin (BTC) and Ether (ETH), among others.
- The term "Customer"/"User"/"You" refers to any individual who uses or accesses the Platform for trading in Cryptos.
- "Customer Due Diligence (CDD)" is the process of identifying and verifying the identity of the customer using a reliable and independent source of documents, data, or information.

- "Officially Valid Document/OVD" refers to documents such as passport, driving license, proof of possession of an Aadhaar Number, or voter's identity card issued by the Election Commission of India. For this definition, "Aadhaar Number" means an identification number as defined under the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.
- The term "Person" refers to an individual who is an Indian citizen-resident and is above the age of eighteen (18) years.
- A "Politically Exposed Person" (PEP) is an individual who is authorized to perform prominent public functions in a country, such as governors of the state, members of Parliament, military officers, senior government and judicial executives, and heads of local bodies such as municipal corporations, among others. Family members or close relatives of such individuals may also be considered as PEPs.
- The term “Suspicious Transaction” means any transaction, including attempted transactions on the Platform, which, at SunCrypto’s sole discretion:
  -gives rise to a reasonable suspicion that it may involve proceeds of a crime or an offense, irrespective of the value involved; or
  -appears to be made under circumstances of unusual or unjustified complexity, or in violation of any Applicable Law; or
  -appears to have no economic rationale or legitimate purpose; or
  -gives rise to a reasonable suspicion that it may involve financing of activities related to terrorism. Terrorism includes transactions involving funds suspected to be linked or related to, or used for terrorism, terrorist acts, or by a terrorist, terrorist organization, or those who finance or attempt to finance terrorism.
- The term “User Account” or “SunCrypto Account” means the account created on the Platform, through which the User provides instructions for Crypto trading to SunCrypto.

KNOW YOUR CUSTOMER NORMS:

(i.) The fundamental principle for identifying any individual who opens and operates a User Account is KYC, which stands for 'Know Your Customer'. This method enables institutions to effectively confirm and authenticate the identity of a customer.

(ii.) Customer identification involves verifying the documents and information provided by the customer. The objectives of KYC are as follows:

-Ensuring appropriate customer identification.

-Monitoring transactions of a suspicious nature.

-Ensuring that the proposed customer is not an undischarged insolvent.

-Reducing the risk of fraud.

-Preventing the opening of Benami accounts with fictitious names and addresses.

-Identifying and removing undesirable customers.

DECLARATIONS AND OBLIGATIONS:

- Declarations and Disclosure of Information by the Platform:

(i.) When a User chooses to trade using the Platform or applies to be a Customer, SunCrypto will verify their identity. SunCrypto will collect and request documents and data from the User as necessary to establish and verify their identity for KYC purposes and to identify any Suspicious Transactions on the Platform. All information provided by the User for KYC and customer identification purposes, as well as information on Suspicious Transactions, must be accurate and up-to-date. SunCrypto may also use various software, technology, or other means, either directly or through service providers/vendors, to verify the User's identity and the information provided. By using the Platform, the User consents to such identity verification and KYC checks.

(ii.) SunCrypto will request documents and data for KYC and customer identification purposes from the User and will access and use them in accordance with this Policy, Applicable Laws, and the Privacy Policy accessible at https://suncrypto.in/privacy-policy.

(iii.) SunCrypto will make reasonable efforts to verify the identity, address, and other details and documents submitted by the Users, either directly or through third-party vendors/service providers, using legally and operationally tenable methods, including but not limited to:

a. Verification of PAN/e-PAN through government sources; or
b. Verification of Masked/Offline Aadhaar/Proof of Possession of Aadhaar under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or
c. Verification of Passport issued under the Passports Act, 1967; or
d. Verification of Voter ID card issued by the Election Commission of India; or
e. Any additional documents that the Platform may require from time to time.

(iv.) As a User, you agree to provide the necessary documentation and information for KYC checks promptly to create and maintain your Platform Account, through which you may instruct the Platform.

(v.) Your failure to provide the required KYC documents, identification documents, or information may limit or completely prevent your use of the Platform and related services.

(vi.) SunCrypto may modify the list of required documents, verifications, and information at its sole discretion without prior notice.

(vii.) SunCrypto has the right to examine or request additional information and documents to verify your identity and financial position, including the sources

of your funds and the details of the Crypto wallet from which you transferred or received any Crypto.

(viii.) If you do not comply with the requirements, SunCrypto will not allow you to create or operate the User Account or carry out Crypto transactions through the Platform.

(ix.) You agree to provide any additional documents required by SunCrypto immediately upon receiving a written request, to comply with Applicable Laws, SunCrypto policies, or a request from any law enforcement authority.

(x.) You further guarantee that you will provide accurate, complete, and genuine KYC documents, information, and data to SunCrypto, its delegates, agents, or representatives.

(xi.) If SunCrypto considers any transaction or series of transactions to be a Suspicious Transaction or reasonably suspects that it may involve proceeds of crime or be used for illegal activities, or if SunCrypto receives requests from any banking partner/payment system provider or participant/statutory/regulatory/supervisory/law enforcement authority, SunCrypto will report such Suspicious Transactions to the Authorities, as well as use, retain, and share your personal data, documents, and information with the Authorities.

(xii.) In such circumstances, SunCrypto may block and freeze your access to the Platform and your SunCrypto Account and increase future monitoring of your User Account. You, as a User, warrant to provide all necessary assistance, support, and cooperation, including additional documents, to verify identity or transaction details.

(xiii.) SunCrypto does not allow the opening or maintenance of anonymous User Accounts, accounts created under fictitious names, or more than one account per person whose identity has not been revealed or verified.

- User Responsibilities:

(i.) By using the Platform, you agree to comply with this KYC/AML Policy, as updated periodically, and all applicable laws and regulations, and to use the Platform exclusively for lawful purposes.

(ii.) You must not use the Platform to engage in any illegal, criminal, or anti-national activities, or to finance such activities under any circumstances.

(iii.) Impersonation of another person or misrepresenting yourself on the Platform is strictly prohibited.

(iv.) You warrant and undertake that you will not participate in any Benami transactions or transactions that violate any Applicable Laws, this Policy, or any other policy or directive issued by SunCrypto from time to time.

POLICY FOR CUSTOMER APPROVAL" OR "PROCEDURE FOR CUSTOMER ENDORSEMENT:

- Opening a SunCrypto Account

(i.) Any Indian resident can open a SunCrypto Account within India's geographical territory and jurisdiction.

(ii.) To activate their SunCrypto Account, the User must provide the following:

a. Permanent Account Number (PAN) issued by the Income Tax Authorities,

b. Documents for identification and proof of residence (Aadhaar/Voter ID/Passport),

c. Live selfie from the camera.

(iii.) After the account opening process, the User needs to add and verify their bank account/UPI ID to make INR deposits/withdrawals.

(iv.) The documents/data mentioned above will establish the identity of the User, but additional information may be collected while opening the SunCrypto Account, such as:

a. Annual income,

b. Occupation,

c. Politically Exposed Person (PEP) status,

d. Trading experience, and

e. Marital status.

(v.) SunCrypto will activate the User's SunCrypto Account only when all the documents and information mentioned above or any additional information requested by SunCrypto have been verified to its satisfaction.

(vi.) SunCrypto will maintain an audit trail of any upload/modification/download.

MEASURES FOR PLATFORM SECURITY:

(i.) Before registering a SunCrypto Account, we make reasonable efforts to ensure that:

a. Users are not accessing the Platform under an anonymous or fake name.

b. No SunCrypto Account is made operational and the User is not allowed to use our services if we are unable to verify the User's identity, obtain required documents or if the documents/information provided by the User are not reliable or if the User does not cooperate with us.

c. We follow CDD (Customer Due Diligence) procedures before opening any account or executing trades.

d. The User's identity does not match any person with a known criminal background or any association/relationship with banned entities/persons such as individual terrorists or terrorist organizations, etc.

(ii.) Users are not allowed to act on behalf of another User and can only transact on SunCrypto's platform using their own account, funds, and for their own benefit. Users cannot create any anonymous accounts, accounts under a fake name, or accounts on behalf of undisclosed or unverifiable persons.

(iii.) SunCrypto may review the User's SunCrypto Account and transactions for any suspicious activity or if requested by authorities. If we find any suspicious activity, or if we receive instructions from authorities, we may suspend, freeze, block, disable, or terminate the User's SunCrypto Account.

(iv.) SunCrypto may refuse to open any new accounts, suspend or terminate existing User Accounts after giving notice, or refuse to process any transactions on the Platform if we are unable to ensure compliance with any of the aforementioned conditions due to non-cooperation by the User, or if the details provided by the User are found on any Sanctions Lists, or are unreliable or unverifiable to SunCrypto's satisfaction

(v.) SunCrypto shall take reasonable measures to ensure that it does not hold any accounts in the names of individuals listed in the watchlists, sanctions lists, or other international agreements approved by the United Nations Security Council (UNSC) or other international agencies suspected of having terrorist links

PROCEDURE FOR CUSTOMER VERIFICATION/AUTHENTICATION:

SunCrypto's Know Your Customer (KYC) and data collection procedures aim to achieve proper customer identification, which involves conducting Customer Due Diligence (CDD). To establish the identity of each User and the purpose of their transactions, SunCrypto may require adequate information at various stages of accessing the Platform, including but not limited to registering a User's account, periodic reviews, transaction executions, and doubts regarding the authenticity or sufficiency of previously obtained identification data.

(i.) User identification

Establishing the identity of a User is a crucial requirement for registering and opening a SunCrypto Account. SunCrypto ensures that verification and due diligence of a User are completed satisfactorily before allowing any SunCrypto Account on the Platform.

(ii.) Definition of Identity

Identity refers to a collection of characteristics that distinctly identify a 'natural' or a 'legal' person. Identifiers are the attributes that help establish a person's unique identity and can be categorized into two types: Primary and Secondary.

a. Primary Identifiers: These include the person's full name, Date of Birth, PAN number, and Passport number/Voter Identity Card/Driving License, as they aid in precisely identifying the person.

b. Secondary Identifiers: These comprise information such as address, location, Nationality, and other similar factors that assist in further refining the identity. The User identification process is an ongoing exercise that does not terminate at the point of application.

(iii.) Definition of Identification

Identification is the process of determining the true identity of a person, which includes verifying the information provided by the User that covers the elements of their identity, such as name and address. In the context of KYC, identification means verifying who a person claims to be. In order to carry out CDD, the following features and documents need to be obtained from an individual to establish their identity:

(a) Permanent Account Number (PAN) or its digital equivalent, e-PAN

(b) A certified copy of an Officially Valid Document (OVD) or its digital equivalent, which contains the details of identity and address. Officially Valid Document (OVD) refers to documents such as Passport, Aadhaar card, Voter's Identity Card, or any other document required by SunCrypto, at its sole discretion and from time to time.

PERIODIC KYC UPDATION:

SunCrypto performs periodic KYC updates for its Users using processes and documents chosen at its sole discretion. The frequency and methods for periodic KYC updates are determined based on a risk-based approach. The following processes are adopted for different situations:

a. No change in KYC information: If there is no change in the User's KYC information, SunCrypto may obtain a self-declaration from the User through their registered email and mobile number.

b. Change in address: If there is only a change in the User's address details, SunCrypto may obtain a self-declaration of the new address along with valid proof through the User's registered email and mobile number.

c. Change in contact information: If there is a change in the User's contact details, the User can update the details by providing valid proof of the change and demonstrating ownership of the SunCrypto Account for which the details are to be updated.

CUSTOMER DUE DILIGENCE (CDD) TYPES:

There are two types of Customer Due Diligence (CDD) that SunCrypto may employ, depending on the level of risk associated with the customer.

(i.) Basic Due Diligence entails collecting and verifying identity proof, address proof, and a photograph to confirm the user's identity. This is carried out by examining the information and documents submitted by the User.

(ii.) Enhanced Due Diligence (EDD) involves additional diligence measures that go beyond Basic Due Diligence. EDD measures may include, but are not limited to, checking whether a User is a Politically Exposed Person (PEP) or has links to terrorist activities or groups, monitoring the account activity of such users, and so on.

SunCrypto shall perform Basic Due Diligence, Enhanced Due Diligence, or any other type of due diligence activity or measures that it deems necessary for a User to register or use the Platform, in its sole discretion and/or in accordance with Applicable Laws."

ANTI-MONEY LAUNDERING (AML) STANDARDS:

According to the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, Regulated Entities (REs) are required to follow certain customer identification procedures when registering with the Platform and conducting transactions, including establishing account-based relationships and monitoring transactions. Although SunCrypto is not an RE, it has voluntarily adopted the KYC/AML/CFT processes under the aforementioned Act and Rules.

SunCrypto is committed to fighting money laundering and terrorist financing and has implemented processes to prevent such activities on its Platform.

SunCrypto has implemented certain steps with an objective to prevent any money laundering activity and/or terrorist financing on the Platform. Such processes being implemented are exhaustive in nature and are subject to change as required under any Applicable Law and/or as per SunCrypto’s sole discretion.

CONTINUOUS TRANSACTION MONITORING:

It is crucial to monitor and supervise SunCrypto Accounts for any suspicious activities.

(i.) SunCrypto will conduct ongoing due diligence by monitoring a User's SunCrypto Account activities through the Platform to ensure that they are in line with their risk profile and source of funds.

(ii.) If SunCrypto detects any suspicious transactions, doubts the adequacy or veracity of previously obtained User identification data, or suspects money laundering or financing of terrorism, it may review due diligence measures, verify the User's identity again, and request additional information. Users must provide all requested information.

(iii.) Monitoring customer activity and transactions is essential to assess risk, know customers, and prevent financial crimes. However, the level of monitoring depends on the customer's risk category. High-risk accounts require more intense monitoring.

(iv.) Certain transactions must be monitored, and SunCrypto may freeze or suspend any SunCrypto Account, block User access, or terminate accounts as determined by SunCrypto in its sole discretion. Transactions that require close monitoring include very high account turnover inconsistent with the balance maintained, complex and unusually large transactions, and unusual patterns that are inconsistent with the User's normal and expected activity and lack an apparent economic rationale or lawful purpose.

(v.) SunCrypto may use alerts when transactions are inconsistent with risk categorization. SunCrypto will utilize updated customer profiles as part of its effective identification and reporting of suspicious transactions.

RISK MANAGEMENT:

(i.) To prevent risks such as fraud, money laundering, inadvertent overdrafts, and Benami/fictitious accounts, customer identification is a critical requirement for opening an account.

(ii.) Failure to comply with transaction monitoring requirements, exceeding threshold limits, and not recording transactions may lead to intentional splitting/structuring of transactions to evade taxes, money laundering, and financing of terrorist activities.

(iii.) SunCrypto periodically conducts a Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment to identify, assess, and mitigate money laundering and terrorist financing risks for Users, countries or geographic areas, and products, services, transactions, or delivery channels that is consistent with any national risk assessment conducted by a body or authority duly notified by the Central Government.

(iv.) As a best industry practice, SunCrypto categorizes Users into low, medium, and high-risk categories based on their assessment and risk perception. The customer profile should contain information relating to the customer's identity, social/financial status, nature of the business activity, and risk categorization shall be undertaken based on these parameters.

(v.) User accounts should be periodically updated based on their risk category. Unless required under this Policy, Applicable Law, or for complying with any request of Authorities, the periodicity of such updating should not be less than once in five (5) years for low-risk category customers and not less than

once in two (2) years for high and medium risk categories. SunCrypto reserves the right to change the periodicity at any time and from time to time at its sole discretion.

(vi.) When considering customer identity, SunCrypto may also factor in the ability to confirm identity documents through online or other services offered by the issuing authorities. The customer profile is confidential, and details contained therein shall not be divulged for cross-selling or any purposes other than those specified in this KYC/AML Policy, Terms of Service, Privacy Policy, or any other policies of SunCrypto made available on the Platform or otherwise informed to the User from time to time.

(vii.) SunCrypto assesses each customer's risk categorization based on their experience, expertise, judgment, assessment, and risk perception of the customer and not merely based on any group or class they belong to.

(viii.) SunCrypto's risk assessment shall be reasonably documented, consider all relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied, be kept up-to-date, and be available to competent authorities and self-regulating bodies/Authorities if and as required under Applicable Laws.

PERIODIC UPDATION OF KYC'S:

SunCrypto carries out periodic updation of KYC for Users at intervals and through processes/documents determined at its discretion. The approach for periodic updation is based on the risk of the User, as described earlier.

a. No change in KYC information: If there is no change in the KYC information, SunCrypto obtains a self-declaration from the User through their registered email and mobile number.

b. Change in address: If there is a change in the User's address details only, SunCrypto obtains a self-declaration of the new address from the User through their registered email and mobile number, along with valid proof for the change.

c. Change in contact information such as phone number or email address: If there is a change in the User's contact details, the User can update the details with SunCrypto by providing valid proof of change.

d. Change in any other information: If there is any change in the information provided during onboarding or periodic updates, the User should inform SunCrypto with valid proof of change at compliance@suncrypto.in".

INTERNAL CONTROLS MECHANISMS:

Record Preservation / Management:

(i.) SunCrypto shall ensure that all information received for identification or due diligence purposes is used in accordance with its applicable terms and conditions. It shall also take necessary and reasonable steps to maintain, preserve, and report User information in accordance with its internal policies and standard operating procedures.

(ii.) SunCrypto shall maintain the confidentiality, security, and protection of all User information collected or created by SunCrypto in compliance with Applicable Law, and prevent unauthorized access, use, disclosure, publication or display of such information.

(iii.) SunCrypto shall keep records in the form of books or stored in a computer, of all User identity proof, documents and information provided, as well as all transactions undertaken by the User on the Platform, in compliance with Applicable Laws and good industry practices.

(iv.) SunCrypto shall maintain and report to the Authorities records of:

a. KYC details, documents, and data of all Users who open a User's Platform Account on the Platform;
b. KYC details, documents, and data of all Users who undertake a transaction on the Platform; or
c. Your transactions on the Platform.

(v.) Regardless of anything to the contrary contained in the Terms of Use or Privacy Policy, any information obtained during due diligence measures or the creation and maintenance of the SunCrypto Account shall be maintained for as long as the account is operational and for a period of 5 (Five) years from the date the SunCrypto Account ceases to exist or as specified under any Applicable Law/Authority.

(iv.) Upon request, SunCrypto will provide authorities with access to identification records and transaction data.

(v.) In the event that SunCrypto:

a. suspects that transactions may be involved in money laundering or terrorist financing, or

b. doubts the sufficiency or accuracy of previously obtained identification data,

appropriate actions will be taken to review the due diligence measures performed by the Platform or the information gathered (regarding the purpose and intended nature of the business relationship) from the User.

Employees Training on KYC's:

(i.) SunCrypto will implement screening mechanisms during its personnel recruitment and hiring process to ensure that high standards are maintained.

(ii.) SunCrypto will provide adequate training programs to its staff on KYC/AML/CFT policy. The training focus may vary depending on the employee's role, such as frontline staff, compliance staff, risk management staff, audit staff, and staff dealing with new customers.

(iii.) SunCrypto may establish policies and FAQs, Do's and Dont's to answer Users' queries and questions and ensure their satisfaction while seeking information in furtherance of the Policy.

(iv.) SunCrypto has made every effort to ensure that this Policy adheres to applicable laws. The invalidity or unenforceability of any part of this Policy will not affect the validity or enforceability of the rest of this Policy. This Policy applies only to information collected by SunCrypto through the Platform and does not apply to any other information.

PRINCIPAL OFFICER:

SunCrypto has designated a Principal Officer, Mr. Pramod Yadav, to oversee compliance with the obligations outlined in this Policy and under relevant laws. Mr. Yadav can be contacted at compliance@suncrypto.in .

If you have any inquiries or complaints regarding this Policy or if you possess knowledge of any unlawful or suspicious activity involving a User, please contact us at compliance@suncrypto.in