KYC/AML Policy
Version 2.0

Know Your Customer and Anti-Money Laundering Policy
CoinSwitch Exchange

This Know Your Customer ("**KYC**") and Anti-Money Laundering ("**AML**") Policy ("**KYC/AML Policy**") details the KYC and AML requirements to access and use our exchange (collectively "**Platform**"), operated under the brand name of "CoinSwitch Exchange", which provides an online platform to connect buyers and sellers of Virtual Digital Assets ("**VDA**"/ "**Crypto**"/ "**Crypto Assets**").

The Platform is managed and operated by NextGenDev Solutions Private Limited, a private company incorporated under the Companies Act 2013 (hereinafter referred to as "**Us**"/"**We**"/"**NGD**"), which is a Reporting Entity under the Prevention of Money Laundering Act, 2002 ("PMLA"). NGD reserves the right, at its sole discretion, to change, modify, add or remove portions of this KYC/AML Policy, at any time without any prior written notice. It is the User's responsibility to review the KYC/AML Policy periodically for any updates/changes. This KYC/AML Policy is also subject to the Terms of Use and Privacy Policy.

NGD is vigilant in the fight against money laundering and under its best judgment implements processes not allowing any person or entity to use the Platform for money laundering and terrorist financing activities.

1. Definitions

1.1 "Applicable Law" shall mean any applicable statute, law, regulation, ordinance, rule, judgment, order, decree, by-law, approval from the concerned authority, government resolution, order, directive, guideline, policy, requirement, or other governmental restriction in force in India, including without limitation the Foreign Exchange and Management Act, 1999 and regulations thereunder, Prevention of Money Laundering Act 2002 ("PMLA"), the Prevention of Money Laundering (Maintenance of Records) Rules 2005 ("PMLR"), AML & CFT Guidelines For Reporting Entities Providing Services Related To Virtual Digital Assets ("AML Guidelines"), as issued by the Financial Intelligence Unit – India ("FIU-IND"), and various applicable guidelines, rules and regulations of the Computer Emergency Response Team, India ("CERT-In"), replaced and updated from time to time;

1.2 "Beneficial Owner": The beneficial owner shall be determined as under—
(a) where the client is a company, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means. Controlling ownership interest" means ownership of or entitlement to more than ten per cent. of shares or capital or profits of the company; and "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements;
(b) where the client is a partnership firm, the beneficial owner is the natural person(s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than ten per cent. of capital or profits of the partnership, or who exercises control through other means; "Control" shall include the right to control the management or policy decision;
(c) where the client is an unincorporated association or body of individuals, the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than fifteen per cent. of the property or capital or profits of such association or body of individuals;
(d) where no natural person is identified under (a) or (b) or (c) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

(e) where the client is a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen per cent. or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership; and
(f) where the client or the owner of the controlling interest is an entity listed on a stock exchange in India, or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a subsidiary of such listed entities, it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

1.3 "Designated Director" means a person designated by NGD to ensure overall implementation of the obligations imposed under chapter IV of the PMLA and the PMLR;

1.4 "Principal Officer " means an officer designated by NGD to ensure compliance with the obligations imposed under chapter IV of the PMLA and the PMLR;

1.5 “Crypto(s)” are Virtual Digital Assets (“VDA”) and refer to a cryptographically secured digital representation of value or contractual rights that uses distributed ledger technology and can be transferred, stored or traded electronically using the Platform, including but not limited to bitcoin and ether;

1.6 “Customer”/“User” shall mean any Person or Organization using/accessing the Platform or interacting with it in any manner for buying, selling, depositing or withdrawing Crypto(s);

1.7 “Customer Due Diligence (CDD)” means identifying the Customer and verifying their identity by using a reliable, independent source of documents, data, or information;

1.8 “Officially Valid Document (OVD)” means the Passport, the Driving License, proof of possession of an Aadhaar Number, or the Voter’s Identity Card issued by the Election Commission of India. For the purpose of 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.

OVDs for legal entities shall mean:
(a) company –
i. certificate of incorporation;
ii. memorandum and articles of association;
iii. Permanent Account Number (“PAN”) of the company;
iv. a board resolution and power of attorney granted to its managers, officers or employees to transact on its behalf;
v. documents relating to beneficial owners, the managers, officers or employees, as the case may be, holding an attorney to transact on the company’s behalf.

(b) partnership firm –
i. registration certificate;
ii. partnership deed;
iii. PAN of the partnership firm; and
iv. documents relating to beneficial owners, the managers, officers or employees, as the case may be, holding an attorney to transact on the partnership firm’s behalf.

1.9 “Person” means an individual who is above eighteen (18) years of age and an Indian citizen.

1.10 "Organization" means any entity registered in India that carries out the function of a business, and has a separate legal existence from the individuals associated with it.

1.11 "Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions by a foreign country, including the Heads of States/Governments, senior politicians, senior government or judicial or military officers, senior executives of state-owned corporations and important political party officials. A User could also qualify as a PEP if the User is a family member or a close relative of such an individual. PEP also includes "PEP Entity", meaning any corporation, business or other entity that (a) has been formed by, or for the benefit of, a PEP, (b) has a key controller who is a PEP (e.g., the PEP exercises actual or effective control over the entity); or (c) has a PEP that is the ultimate beneficial owner.

1.12 "Virtual Digital Assets (VDA)" means any information or code or number or token (not being Indian or foreign currency), a non-fungible token or any digital asset as defined under Section 2(47A) of Income Tax Act, 1961.

1.13 Permanent Account Number (PAN) is issued by the Indian Income Tax Department to help uniquely identify tax payers. e-PAN is an electronically issued PAN which is digitally signed.

2. Customer Acceptance Policy (CAP)

2.1. KYC norms

2.1.1. KYC means to 'Know Your Customer' which is an effective way for an institution to confirm and thereby verify the authenticity of a customer. KYC is the key principle for the identification of any individual or Organization interacting and/or transacting with NGD. This KYC principle applies to the Users of the Platform, and is also being undertaken to comply with the "Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet" issued by the Ministry of Electronics and Information Technology (MeitY) - Indian Computer Emergency Response Team (CERT-In) on 28 April, 2022.

2.1.2. The Customer/User identification includes identification and verification of the Customer's identity on the basis of documents and information provided by the Customer. The objectives of KYC are as under:

(a) To ensure appropriate Customer identification and comply with all Applicable Law(s),
(b) Monitor all transactions,
(c) Satisfy that the proposed Customer is not an undischarged insolvent,
(d) Minimize frauds,
(e) Avoid transacting with individuals or entities having fictitious names and addresses, and
(f) Avoid undesirable Customers.

2.2. Onboarding Procedures

2.2.1. Any applicant individual or Organization can apply to access the Platform, post which NGD will review the application and decide whether access should be granted.

2.2.2. The applicant has to provide the following and if the applicant is an Organization, then all the associated significant individuals (beneficial owners, controllers, CEO, principal officers, promoters,

authorized persons) and associated Organization (legal entity owners) as well before they can access the Platform:

(a) PAN given by Indian Income Tax Authorities,
(b) Corporate identification number for entities,
(c) Address and business activity,
(d) Bank account number,
(e) Documentation supporting the information provided,
(f) Declarations.

2.2.3. The applicant's access to the Platform will only be made operational to avail our services when such documents, information as mentioned above, or any other additional information as requested by NGD has been verified as per the satisfaction of NGD.

2.3. NGD shall verify the provided information and documentation, and maintain an audit trail of any upload/modification/download.

2.4. Safeguard measures taken by NGD

2.4.1. Before accessing the Platform, We on a reasonable efforts basis ensure that:

(a) Users are not accessing the Platform under an anonymous or fictitious name.

(b) User is not allowed to avail our services in an event if we are unable to apply appropriate CDD measures, i.e. verify the User identity and/or obtain documents required or non-reliability of the documents/information furnished to NGD, either due to non-cooperation of the User or non-reliability of the documents/information furnished by the Customer.
(c) No access is granted to the Platform or trades are executed without following CDD procedure.
(d) The identity of the User and any of its related individuals do not match with any person with a known criminal background or having any association/ relationship with banned entities/ persons such as individual terrorists or terrorist organizations etc., or having any connection with any high-risk jurisdiction.

2.4.2. Users are not permitted to act on behalf of anyone else and can only access the Platform on their own, with their own funds/assets, and for their own benefit.

2.4.3. NGD at its sole discretion shall review the User's information and documents provided and transactions for any suspicious activity or in an event if NGD receives a request for the same from Authorities and based on NGD's judgment or instruction from Authorities such User's access to the Platform shall be suspended, frozen, blocked, disabled, or terminated.

2.4.4. NGD shall, in its sole discretion, refuse to provide access to the Platform to new Users, suspend or terminate access to the Platform to existing Users after giving due notice, or refuse to process any transactions on the Platform if it is unable to ensure compliance with any of the aforementioned conditions, either due to non-cooperation by the User or due to the details provided by the User being found enlisted on any Sanctions Lists or unreliable or unverifiable to NGD's satisfaction.

2.4.5. *Requirements/obligations under international agreements & Communication from international agencies*: NGD shall reasonably ensure that it does not have any association with individuals appearing in

the lists of individuals and entities, suspected of having terrorist links, which are approved by and periodically circulated by the United Nations Security Council, other watchlists and sanctions lists.

3. Customer Identification Procedure (CIP)

One of the objectives of the KYC and data/information collection norms being carried out by NGD is to ensure appropriate Customer Identification. Customer Identification means undertaking the process of CDD. NGD shall need to obtain sufficient information necessary to establish, to its satisfaction, the identity of each User, whether regular or occasional, and the purpose of the intended nature of the transactions being executed on/ through the Platform.

Customer Identification Procedure is carried out at different stages while the Platform is accessed by the User and is not limited to instances when:

(a) Applying to access the Platform,
(b) Periodic review of a User's information and documents,
(c) Any transaction is being executed by the User on the Platform, and/or
(d) NGD has a doubt about the authenticity/veracity or the adequacy of the earlier obtained User Identification data.

3.1. User identification

Identification of a User is an important prerequisite for accessing the Platform. No access is allowed on the Platform unless verification and due diligence of said User is successfully completed by NGD.

3.1.1. *What is Identity?*

Identity generally means a set of attributes that together uniquely identify a 'natural' or a 'legal' Person. The attributes which help in the unique identity of a 'natural' or 'legal' Person are called identifiers. Identifiers are of two types: a.) Primary and b.) Secondary.

(a) Primary Identifiers: On a non-exhaustive basis means and includes the name (in full), date of birth, PAN number, and passport number/voter identity card / other govt.-issued identification document as they help in uniquely establishing the identity of the Person.

(b) Secondary Identifiers: On a non-exhaustive basis means and includes address, location, nationality, and other such identification, as they help further refine the identity. User identification does not start and end at the point of application but it is always an ongoing exercise.

In this case, Identity also applies to Organizations that wish to access the Platform. For them, the identifiers are as follows:

(a) Primary Identifiers: On a non-exhaustive basis means and includes the name (in full), Date of Incorporation, PAN number, and Government-issued corporate identification number as they help in uniquely identifying the Organization.

(b) Secondary Identifiers: On a non-exhaustive basis means and includes address, location, business activity, key personnel details and other such identification, as they

help further refine the identity. User identification does not start and end at the point of application but it is always an ongoing exercise.

3.1.2. *What is Identification?*

Identification is the act of establishing who a Person is:

(a) In the context of KYC, identification means establishing who a Person or Organization purports to be.

(b) This is done by recording the information provided by the User covering the elements of their identity (i.e. name, and the address at which they can be located).

(c) For undertaking CDD, the OVDs shall be obtained from a User while establishing a relationship.

3.1.3. *What is Verification?*

Verification of identity is the process of proving whether a Person or Organization actually is who they claim to be. In the context of KYC, verification is the process of seeking satisfactory evidence of the identity of those with whom NGD does business. This is done by carrying out checks on the correctness of the information provided by the Customer.

3.1.4. *Process of validation of documents through video-KYC*

In scenarios where the document provided by a User has some issues and cannot be validated using the automated solutions NGD has in place, a video-KYC might be required from the User to validate the identity and authenticity of the document/information submitted by them. KYC of individuals associated with the Organization that are required to furnish OVDs or any other documents might be done with video-KYC. We would also use the video-KYC process while performing enhanced due diligence wherever required.

3.1.5 Customer Due Diligence (CDD)

CDD would be performed in accordance with the risk category of the Customer, as follows:

a. Basic Due Diligence means the collection and verification of identity proof and address proof to establish the identity of the User. This is done on the basis of the documents and information submitted by the User. This due diligence would be performed on all Users.

b. Enhanced Due Diligence (EDD) means additional diligence measures undertaken over and above the Basic Due Diligence, in cases of High-risk Users. Steps under EDD shall include but will not be limited to requesting for additional information and documentation to support any information provided earlier (e.g. bank statements or other financial records for verifying the source of funds information), additional background checks and research to validate the true identity of a User, monitoring the activity of such Users, requesting for additional information and documentation, conducting in-person visits etc.

NGD shall conduct Basic Due Diligence, EDD, or any other due diligence activity or measures which under its sole discretion and/ or under Applicable Laws is required for a User registering or

using the Platform. NGD reserves the right to request for additional information and documentation, as required.

4. Anti-Money Laundering Standards

In terms of the provisions of Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, as amended from time to time, and the AML Guidelines, Reporting Entities (REs) are required to follow certain customer identification procedures while registration with the Platform and undertaking a transaction either by establishing an account-based relationship or otherwise and monitor their transactions. NGD is also registered with the FIU-IND as a Reporting Entity (RE), and accordingly has taken steps to adopt the KYC/AML/CFT processes under the aforementioned AML Guidelines.

4.1. Steps taken to prevent Money-Laundering activities and Terrorist Financing

NGD has implemented steps as described below 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 NGD's sole discretion.

6. Declarations and Obligations

6.1. Declarations and Disclosure of Information by NGD

6.1.1. NGD will identify and verify User's identity at the time the User opts to trade using the Platform or apply to be a Customer. To this effect, NGD shall collect such documents and data, as may be reasonably requested by NGD from time to time, to establish and verify the identity of the User / for KYC purposes / to establish and verify the nature of any transaction undertaken on the Platform. NGD shall also use/deploy various software and/or technology, either directly or through its service providers/vendors to establish and verify User's identity and/or the documents/information provided by the User.

6.1.2 The documents and data for KYC and Customer identification purposes shall be requested from the User and shall be accessed and used by NGD as per this Policy, the Applicable Laws, and the Privacy Policy.

6.1.3 NGD shall endeavor to verify, either itself or through third-party vendors/service providers, the identity and address of the Users along with the other details and documents submitted by the User as may be legally/operationally tenable, including but not limited to using the following methods:

(a) PAN/e-PAN verification through government sources; or
(b) Masked/Offline Aadhar/Proof of Possession of Aadhar under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016; or
(c) Passport issued under the Passports Act, 1967; or
(d) Verification of Voter ID card issued by the Election Commission of India; or
(e) Constitutional documents for Organizations (Memorandum/Articles of Association / Agreements per the entity type / By-laws); or
(f) Corporate ownership documents for Organizations (organizational chart / shareholding structure chart); or
(g) Any other / additional document may be required by NGD from time to time.

6.1.4 In case the User fails to provide the requisite KYC documents or any identification documents or information as requested by NGD, NGD shall hinder or completely restrict User's use of the Platform and

the related services. This includes but is not limited to not crediting the deposited Crypto and not completing the withdrawal processing of Crypto if the required information to comply with the Travel Rule (see 3.1.7 below) is not available, or if the regulatory checks for Travel Rule are not satisfied.

6.1.5 The list of documentation (as mentioned under clause 1.5), verification, and information may be amended by NGD by way of a notification/intimation, in its sole discretion from time to time, without a prior notice.

6.1.6 NGD reserves the right to examine or request additional information and documents to establish User's identity, and financial position, including sources of User's funds and/or details of the Crypto wallet or similar accounts from which User transfers / to where User receives any Crypto, and User shall provide all assistance and cooperation in this regard. NGD also reserves the right to verify that any Crypto wallet used to transfer Crypto is operated/based in India. NGD will obtain User's complete Crypto wallet address at the time of on-boarding and if the User fails/refuses to comply with the requirements herein, NGD shall not allow the User to access the Platform or carry out transactions through the Platform.

6.1.7 To comply with the Travel Rule requirements, wherein the originator information needs to be shared with the counterparty exchange in case of withdrawal of VDA by the User, NGD can reach out to the User to obtain additional information, in line with the AML & CFT Guidelines For Reporting Entities Providing Services Related To Virtual Digital Assets ("AML Guidelines"), as issued by the Financial Intelligence Unit – India ("FIU-IND"). NGD can also reach out to obtain the required information to verify beneficiary information in case of deposit of VDA by the User, if the corresponding Travel Rule information is missing/incomplete as received from the originating exchange. The successful completion of such withdrawals and deposits of VDA is subject to the internal Travel Rule and compliance controls implemented by NGD. NGD has integrated with a third-party service provider for implementation of Travel Rule requirements. Travel Rule is applicable for all VDA transfers (deposit and withdrawal), irrespective of the amount or the type of VDA transferred. This process would be per the attached Annexure A.

6.1.8 Additional documents may be requested by NGD to ensure compliance with any Applicable Laws or NGD's policies or a request from any Authorities *(defined below)* immediately.

6.1.9 Where any transaction or series of transactions undertaken by the User are considered as suspicious at the sole discretion of NGD, or NGD reasonably perceives that it is likely to involve proceeds of crime or be used towards any illegal activity, or in an event, if NGD receives requests/requisitions from any banking partner/ payment system provider or participant/ statutory/ regulatory/ supervisory/ law enforcement authority/enforcement authority ("Authorities"), NGD shall report all such transaction(s) to the Authorities, as well as use, retain and share User's personal data, documents, and information available with NGD with the Authorities, and block and freeze, as deemed fit by NGD, the User's access to the Platform, and shall also increase the future monitoring of such Users. NGD may perform multiple User outreaches to collect information and documentation depending on the User's activity and transactions performed.

6.1.10 NGD reserves the right, at its sole discretion, to change, modify, add or remove portions of this KYC/AML Policy, at any time without any prior written notice.

7. Grievance Redressal

7.1. In case of any complaint or queries, Users are directed to the Support team.

8. Risk Management by Periodic Review

8.1. Identification of a Customer is an important prerequisite for beginning a relationship. Non-adherence to this may lead to risks e.g. frauds, money laundering, inadvertent overdrafts, and Benami/fictitious Users.

8.2. NGD will carry out 'Money Laundering and Terrorist Financing Risk Assessment' on an annual basis to identify, assess and take effective measures to mitigate money laundering and terrorist financing risk 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. Reference to the internal process note.

8.3. NGD, as a best industry practice and under its sole discretion categorizes the Users under low, and high-risk categories, based on the assessment and risk perception. NGD should prepare the profile of the Customer which 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.

8.4. All Users' information will be periodically updated based on their risk category. Unless otherwise required under this Policy or under Applicable Law or for complying with any request of Authorities, at present, the periodicity of such updation should not be less than once in one (1) year. NGD reserves the right to change the above periodicity at any time and from time to time in its sole discretion.

8.5. While considering the Customer's identity, the ability to confirm identity documents through online or other services offered by the issuing Authorities may also be factored in. The Customer profile will be a confidential document 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, terms and conditions as agreed between the Customer and NGD through an executed agreement or any other policies of NGD made available on the Platform or otherwise informed to the User from time to time.

8.6. NGD shall take a view on risk categorization of each Customer into low and high-risk categories depending on their experience, expertise in profiling of the Customer based on their understanding, judgment, assessment, and risk perception of the Customer and not merely based on any group or class they belong to.

8.7. The risk assessment carried out by NGD will:

(a) be reasonably documented;
(b) consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied;
(c) be kept up to date; and
(d) be available to competent Authorities and self-regulating bodies/Authorities, if and as required under Applicable Laws.

8.8. <u>Periodic updation of KYC</u>

Periodic updation of KYC of Users is performed at such intervals of time and using such processes/documents as decided by NGD at its sole discretion. A risk-based approach for periodic updation of KYC is adopted, wherein the periodic updation of KYC for all Users is done at least annually or more frequently as per NGD's discretion, to ensure the information and documentation for users is up-to-date.

(a) No change in KYC information: In case of no change in the KYC information, a self-declaration from the User in this regard shall be obtained through User's email id and mobile number registered with NGD.

(b) Change in address: In case of a change only in the address details of the User, a self-declaration of the new address shall be obtained from the User through the User's email id and mobile number registered with NGD along with valid proof to be submitted by the User for the change in such address.

(c) Change in contact information like a phone number or email address: In case of a change in the contact details of the User, the User can reach out to NGD to get the details updated, along with valid proof of change.

(d) Change in shareholding/key management information (for Organizations): In case of a change in shareholding, beneficial ownership, control, key management personnel or any such information provided at the time of onboarding or periodic updates, the User can reach out to NGD to get the details updated, along with valid proof of change.

(e) Change in any other information: In case of any change in the information provided at the time of onboarding or periodic updates, the User should reach out to NGD to get the details updated, along with valid proof of change.

9. Internal Controls

9.1. Preservation of Record / Record Management

9.1.1. NGD will ensure that all information received for the purpose of identification or due diligence is used by it in accordance with NGD's terms and conditions applicable. NGD shall also take necessary reasonable steps for maintenance, preservation, and reporting of User information per the internal policies and standard operating procedures of NGD.

9.1.2. In addition, the confidentiality, security, and protection against access, use, and disclosure (including publication or display) of all information of a User, collected or created by NGD shall be kept in accordance with Applicable Law.

9.1.3. NGD shall collect and maintain records, in the form of books or stored in a computer, of User's identity proof along with all documents and information provided by the User and of all the transactions undertaken by the User on the Platform, as required under the Applicable Laws/good industry practices.

9.1.4. NGD shall maintain and if required, report to Authorities the records of:
(a) the KYC details, documents, and data of all Users who access the Platform;
(b) the KYC details, documents, and data of all Users who undertake a transaction on the Platform; or
(c) User's transactions on the Platform.

9.1.5. Notwithstanding anything to the contrary contained in the Terms of Use or agreement executed between the Customer and NGD or Privacy Policy, any information obtained while undertaking the due diligence measures under this Policy or during registration/creation/ongoing due diligence of User's activities shall be maintained for the duration of the relationship, and for a period of 9 (nine) years from the date the relationship ceases to exist or such longer period as may be specified under any Applicable Law/Authority.

9.1.6. We have taken reasonable effort to ensure that this Policy adheres to the applicable laws. The invalidity or unenforceability of any part of this Policy shall not prejudice or affect the validity or enforceability of the remainder of this Policy. This Policy does not apply to any information other than the information collected by NGD through the Platform.