-INTERNAL / CONFIDENTIAL-

Coinstec's Proposed Procedures Manual

Anti-Money Laundering & Counter-Terrorism Financing Policy

I. Anti Money Laundering ("AML")

Coinstec aims to comply with anti-money laundering ("AML") and counterterrorism financing ("CTF") recommendations in a way that complements business priorities.

It is best practice for Coinstec to ensure that any program being implemented does not explicitly set out full or partial exemptions from AML/CTF requirements, or result in such exemptions in practice. Management places extremely high importance on assisting in discovering any money laundering scheme. These policies are to be read by and adhered to by all employees and officers of the Company. Any employee found not to be adhering to these policies and procedures will face severe disciplinary action. It is the policy of Coinstec and its affiliates to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

II. Personnel

a. AML Compliance Officer

Coinstec shall designate an Anti-Money Laundering Program Compliance Officer ("AML Compliance Officer"), who is also qualified in terms of experience, knowledge and training and to whom any internal report of suspicious transactions must be made.

The AML Compliance Officer will be fully responsible for the Company's AML and CTF program and report to the Board of the Company or a committee thereof any material breaches of the internal AML/CTF policy and procedures and of the AML/CTF laws, codes and standards of good practice.

The duties of the AML Compliance Officer will include monitoring the Company's compliance with AML/CFT obligations, overseeing communication and AML/CTF training for employees.

The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer, will ensure Suspicious Transactions Reports ("STR") are duly filed. All STR records are to be kept for a period of at least seven years.

The AML Compliance Officer will also be responsible for ensuring that the Company has adequate customer identification and verification program in place at all times and in accordance with requirements of the law.

b. Employees

Coinstec shall ensure that all employees are properly trained and fully aware of the Company's AML/CTF policies and procedures. The Company will monitor its employees to ensure that AML procedures are adhered to. Based on the severity and nature of the violation, the employee will be reprimanded and warned that any future violation may result in termination. Coinstec will also perform criminal and disciplinary background checks on all employees before they are hired.

On an annual basis, thereafter, the AML Compliance Officer will also hold internal trainings for all employees. The training will include at a minimum:

1. How to identify red flags and signs of money laundering that arise during the course of the employees' duties.
2. What to do once the risk is identified.
3. What employees' roles are in the Company's compliance efforts and how to perform them.
4. The Company's record retention policy.
5. The disciplinary consequences (including civil and criminal penalties) for non-compliance with the requirements of the applicable legislation.

Employees must report any violation of the Company's AML/CTF compliance program to the AML Compliance Officer, unless the violation implicates the AML Compliance Officer, in which case the employee shall report the violation to senior management. Such reports will be confidential, and the employee will suffer no retaliation for making them.

III. Customer Due Diligence and KYC Procedures

Effective Customer Due Diligence ("CDD") / 'Know Your Customer' ("KYC") measures are essential to the management of money laundering and terrorist financing risk. CDD is identifying the client and verifying their true identity on the basis of documents, data or information obtained from a reliable and independent source both at the moment of starting a business relationship and on an ongoing basis.

Identity is composed by attributes such as names used, date of birth and the residential address of the customer. This information can uniquely identify a natural or legal person. For a natural person, the date of birth should be obtained as an important identifier to support the name. If the customer provides an international passport as evidence of identity, the number, date and country of issue should be recorded (preferably the scan should be maintained on files as well).

The identity must be verified any time a business relationship with Coinstec will be established, an account opened, or a significant one-off transaction is made.

The identity of the following persons should be verified:

1. Clients: sufficient evidence of the identity must be provided to demonstrate that the client is who he/she claims to be.
2. The person acting on behalf of another (such as in a Managed Account Power of Attorney) – both of their identities must be proved by sufficient evidence.

All the following information should be verified with identification documents:

- the named account holder/person in whose name an investment is registered;
- any major (25% and over) beneficial owner of funds being invested who is not the account holder or the named investor;
- the principal controller(s), of an account or business relationship; and
- any intermediate parties (e.g. where the account is managed or owned by an intermediary).

All the signatories that appear in an account and directors who are not the main controllers, should also report their identities and provide adequate documents.

In case of several account holders for one account, evidence of identification should be provided from all the account holders.

Failure or refusal by an applicant to provide satisfactory identification or evidence within a reasonable period of time without adequate grounds may lead to a suspicion that the depositor or investor is involved in money laundering.

IV. Identifications Procedures

Coinstec will make sure that its customer is a real person or organization (natural, corporate or legal entity), by acquiring sufficient identification evidence. When reliance is placed on a third party to identify or confirm the identity of an applicant, the overall legal

responsibility for obtaining satisfactory identification evidence rests with Coinstec. The purpose is to obtain evidence that a person of that name lives at the address given and that the applicant is really that person, or that the company's owner are identifiable and that they can be located at the address provided.

In the case of a foreign customer or clients that cannot be physically present at Coinstec headquarters or local offices, the identification evidence such as the copy of an international passport or a national identity card must be certified by:

- an embassy, consulate or high commission of the country of issue; or a senior official within a bank; or a lawyer or a public notary.

It should be written "original seen"/ "Certified True Copy" on every certified copy of the identification documents.

The photographic evidence of identity should be a good reproduction and when this is not possible the copy of the evidence should be certified as providing a good likeness of the applicant.

The following information should be provided and verified for all private individuals:

- the true full name(s) used; and
- the permanent home address, including postcode.

The fact the customer of the name provided resides at the address given and that he is that person should be confirmed by the information provided, such as a utility bill.

If an applicant has recently relocated to a different address, the previous address should be validated.

The following documents can be used to attest the identification information:

- Personal Identity Documents.
- Current International Passport.
- Residence Permit issued by the Immigration Authorities.
- Current Driving License.
- Inland Revenue Tax Clearance Certificate.
- Birth Certificate/Sworn Declaration of Age.
- Record of Home Visit.
- Confirmation from the electoral register that a person of that name lives at that address.

- Recent utility bill (water, electricity, gas, and internet) – note: it is better to use a physical electricity/municipality bill as utility bill, not a mobile telephone bill.

If those documents can't be provided or are not sufficient, as an alternative or supplementary, the information may be verified electronically by accessing other data sources such as:

- An electronic search in the Electoral Register;
- Access to internal or external account database;
- An electronic search of public records where available.

Besides identity documents, other information must be obtained in the purpose of avoiding money laundering.

In case of doubt and suspicion, customers might be required to provide:

- The legal evidence of the relationship between the signatories and the beneficial owner.
- The origins and the sources of the funds deposited or invested.
- The estimated net worth.
- Information about the occupation or employment of the customer.
- Bank Reference such as detailed on the following page.

BANK REFERENCE

Bank Letterhead

(must contain full address and contact number)

TO WHOM IT MAY CONCERN

Date: …….

REF: Mr. ….

This bank reference hereby confirms that (**name**) of (**full address**) is a client in good standing and has been a client at this bank for the past (**number**) of years.

Sincerely,

(Bank Signing Officer + Stamp)

It must be understood that the amount of information asked, shall vary according to the type of client, the nature of activity with Coinstec and the estimated risk involved.

Certain customers will require a higher level of due diligence:

- Persons residing in or having funds sourced from countries listed as having inadequate anti-money laundering standards or representing high risk for crime and corruption (e.g. Nigeria and other certain countries in Africa, certain countries in Eastern Europe, certain countries in Central America and certain Islamic states –

these lists are distributed on the internet and updated frequently – use them at your own peril);

- Persons involved in business activities or sectors susceptible to money laundering; “Politically Exposed Persons” (PEPs) which means person holding or having held positions of public trust, such as government officials, senior executives of the government, public infrastructure entities, large corporations, defense executives, politicians, important political party officials, etc., as well as their families and close associates.

Coinstec should keep the information in a secure manner and up-to-date.

V. Monitoring Accounts for Suspicious Transactions

Coinstec will monitor a sufficient amount of account activity to permit the identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as “non-cooperative” are involved, or any of the “red flags” identified below. The Company will look at transactions, including trading and wire transfers, in the context of other account activity to determine if a transaction lacks financial sense or is suspicious because it is an unusual transaction or strategy for that customer.

Within a reasonable period of time after an account is opened, the Company will determine whether a customer appears on any such “black list”. If such customer appears on a "black list", the Company will close or freeze the account if any positive match is detected, and the AML/CTF Compliance Officer will need to carefully consider the situation to ensure compliance as far as is possible with any government rules and sanctions that prohibit transactions with certain foreign countries or their citizens.

Several characteristics justify further inspection like:

- the usualness/unusualness of a transaction (regarding to size or frequency); the nature of a transaction;
- the nature of a series of transactions;
- the geographic destination or origin of a payment (to or from a high-risk country); the parties concerned (to or from a person on a sanctions list).

Every measure that will be taken by Coinstec will be compliant with the guidelines issued by competent authorities.

VI. Avoiding Fraud

Whenever clients are using credit cards, Coinstec will ask for scans of both sides of the card and make sure that the scans were not manipulated or altered. The same goes for documentation scans which can be easily manipulated using graphic software suites like PhotoShop. The Company will make sure to receive consent for every transaction from the person stated on the card. E.g. when a client uses its spouse's credit card, Coinstec will receive the spouse's personal consent for the transaction and verify the spouse's identity as described above in order to prevent chargebacks.

For a corporate client, the client should either:

a. provide a certified POA attesting that the signatory can sign and bind the client, or a confirmation from the corporate secretary confirming the same, or:

b. provide a declaration as follows:

"I, ……, hereby personally declare and guarantee that I am entitled to sign on behalf of the corporate entity and I assume full personal liability of the legal consequences should this declaration was incorrect or inaccurate".

Should any questions arise in the ordinary course of business, please feel free to contact us anytime by email or phone. This guide serves as guideline only with no liability for compatibility for a specific regulation.