General Reserve of Digital Assets Limited
KYC POLICY

KNOW YOUR CUSTOMER POLICY

All employees of General Reserve of Digital Assets Limited ("GRDA") are required to comply with the policies and procedures set out in this KYC Policy. When conducting fiduciary activities, reference should be made to relevant requirements stipulated in Hong Kong Ordinance Cap 615 Anti-Money Laundering and Counter Terrorist Financing Ordinance (the "AMLO").

KYC 1
NO ANONYMOUS ACCOUNT

No account should be opened in anonymous or fictitious name or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

KYC2
MUST COMPLETE CUSTOMER DUE DILIGENCE

No account would be opened, if GRDA is unable to apply appropriate customer due diligence measures i.e. GRDA is unable to verify the identity and/or obtain documents required as per the risk categorisation due to non-cooperation of the customer or non-reliability of the data/information furnished to GRDA. While carrying out due diligence it would be ensured that there is no harassment to the customer. The existing account where GRDA is not able to apply appropriate customer due diligence measures may be considered to be closed. The decision to close an account would be taken by the Compliance Officer after giving due notice to the customer, explaining the reasons for such a decision.

KYC3
CUSTOMER DUE DILIGENCE SHOULD NOT BE RESTRICTIVE

While carrying out due diligence, it shall be ensured that the procedure adopted shall not become too restrictive and must not result in denial of GRDA services to general public, specially to those, who are at financial or social disadvantage.

KYC4
CUSTOMER BACKGROUND CHECK BEFORE OPENING A NEW ACCOUNT

Before opening a new account, necessary checks shall be conducted so as to ensure that the identity of the customers/entities/persons associated with the entities does not match with any person with known criminal background or with banned entities such as individual terrorists or terrorist organisations etc. Lists circulated by relevant regulatory authorities of persons with known criminal background or banned entities as well as a list of persons involved in frauds and deliberate default as per information available with GRDA shall be used for this purpose.

KYC5
CUSTOMER INFORMATION MUST BE OBTAINED AT THE TIME OF ACCOUNT OPENING

For the purpose of risk categorisation of customer, the relevant information shall be obtained from the customer at the time of account opening. While doing so, it shall be ensured that information sought from the customer is relevant to the perceived risk and is not intrusive.

KYC6
INDICATIVE RISK CATEGORISATION OF CUSTOMER

Risk perception of different types of customers taking into account the background of the customer, nature of business activity, location of customer/ activity and profile of his/her customers, country of origin, sources of funds, mode of payments, volume of turnover, social and financial status etc. shall be decided based on the relevant information provided by the customer at the

time of account opening. More intensive due diligence would be required for higher risk customers, especially those for whom the sources of funds are not clear. An indicative risk categorization of customers based on customer types is provided at the end of this KYC Policy, which would be reviewed periodically by the KYC Committe of GRDA.

KYC7
ASSESSMENT OF ML/TF RISK OF CUSTOMER

GRDA shall take steps to identify and assess the Money Laundering/ Terrorist Financing risk for customers, countries and geographical areas as also for products, services, transactions, delivery channels. The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. The assessment shall be documented, updated regularly and made available to competent authorities and self-regulating bodies, as and when required.

KYC8
CUSTOMER PROFILING BASED ON RISK CATEGORISATION

A profile for each new customer shall be prepared based on risk categorisation. The customer profile shall contain information relating to customer's identity, social/financial status, nature of business activity, information about customers' business and their location etc. The nature and extent of due diligence shall depend on the risk categorization of the customer. While preparing customer profile, care shall be taken to seek only such information from the customer, which is relevant to the risk category and is not intrusive. The customer profile is a confidential document and details contained therein should not be divulged for cross selling or any other purposes.

KYC9
REQUIRE FURTHER INFORMATION FROM CUSTOMER IF NEEDED

Indicative information to be obtained from the customer at the time of opening of account for the purpose of creating customer profile is given in Identification section. The information to be sought from the customer would be reviewed by KYC Committee from time to time based on the guidelines issued by Company Registry and also depending upon business requirement and composition of the customers.

KYC10
CUSTOMER INFORMATION MUST BE VERIFIED

The documentation requirements for completing the KYC are reviewed by KYC Committe from time to time, based on emerging business needs of GRDA and shall comply with the overall guidelines issued by Company Registry from time to time. Documents for verification of identity is also given in Identification section.

KYC11
CUSTOMER ACCEPTED AFTER IDENTITY VERIFICATION

Customer shall be accepted after verifying their identity as laid down in customer identification procedures. Documentation requirements and other information shall be collected in respect of different categories of customers depending on perceived risk and keeping in view the requirements of AMLO and guidelines issued by Company Registry.

KYC12
MANDATE HOLDER IDENTITY MUST BE VERIFIED

There could be occasions when an account is to be operated by a mandate holder, power of attorney or where an account is to be operated by an intermediary in fiduciary capacity, such

information needs to be obtained while accepting the customer and capture the same in GRDA Customer Profile System.

KYC13
BENEFICIAL OWNER IDENTITY MUST BE VERIFIED

Customer on whose behalf (i.e., Beneficial Owner), the accounts are maintained and operated, such information needs to be obtained while accepting the customer and capture the same in GRDA's Customer Profile System.

KYC14
RELIANCE OF THIRD PARTY INTERMEDIARY CDD WITH CONDITIONS

For the purpose of customer due diligence, GRDA may rely on a third party intermediary subject to the following conditions:

(a) GRDA immediately obtains necessary information of such customer due diligence carried out by the third party;
(b) GRDA takes adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be made available from the third party upon request without delay;
(c) GRDA is satisfied that such third party is regulated, supervised or monitored for, and has measures in place for compliance with customer due diligence and record-keeping requirements in line with the requirements and obligations under the Act;
(d) the third party is not based in a country or jurisdiction assessed as high risk; and
(e) GRDA shall be ultimately responsible for customer due diligence and undertaking enhanced due diligence measures, as applicable.

CUSTOMER DUE DILIGENCE (CDD)

CDD is intended to enable GRDA to form a reasonable belief that it knows the true identity of each customer and, with an appropriate degree of confidence, knows the type of business and transactions the customer is likely to undertake. The CDD requirements are set out in Schedule 2 to the AMLO. Depending on specific circumstances, GRDA may also need to conduct additional measures referred to as enhanced customer due diligence ("EDD") or, alternatively, may conduct simplified customer due diligence ("SDD").

What are GRDA CDD measures ?

The CDD measures applicable to GRDA under section 2 of Part 2 of Schedule 2 to the AMLO are:

(a) identifying the customer and verifying the customer's identity;
(b) identifying and taking reasonable measures to verify the beneficial owner's identity;
(c) obtaining information on the purpose and intended nature of the business relationship (if any) established with GRDA;
(d) if a person purports to act on behalf of the customer:
(e) identifying the person and taking reasonable measures to verify the person's identity;
(f) verifying the person's authority to act on behalf of the customer.

When must GRDA apply CDD ?

GRDA must apply CDD :

(a) before establishing a business relationship with the customer;
(b) before carrying out for the customer an occasional transaction that involves an amount equal to or exceeding an aggregate value of HK$120,000, whether carried out in a single operation or several operations that appear to be linked;
(c) when GRDA suspects that the customer or the customer's account is involved in ML/TF regardless of the levels of transaction of (2) above;
(d) when GRDA doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.

Can CDD be completed after the creation of a business relationship ?

GRDA must complete the CDD process before establishing any business relationship or before carrying out a specified occasional transaction. Where GRDA is unable to complete the CDD process, it must not establish a business relationship or carry out any occasional transaction with that customer and should assess whether this failure provides grounds for knowledge or suspicion of ML/TF and filing a STR with the JFIU.

What if fail to complete verification of identity after business relationship ?

After 60 working days of establishment of a business relationship with a customer:

(a) GRDA must suspend the business relationship and refrain from carrying out further transactions (except to return funds to their sources, to the extent that this is possible)

After 120 working days of establishment of a business relationship with a customer:

(a) GRDA must terminate the business relationship with the customer.
(b) when terminating a relationship where funds or other assets have been received, GRDA must return the funds or assets to the source from which they were received. GRDA can not return the funds or assets to third party, this means that the funds or assets should be returned to the customer/account holder. (not applicable where GRDA is served a restraint order or confiscation order.)

Is re-verification needed ?

GRDA is obligated to take steps from time to time to ensure that customers' information obtained for the purposes of complying with the requirements of sections 2 and 3 of Part 2 of Schedule 2 to the AMLO is up-to-date and relevant. GRDA policy is to undertake periodic reviews of existing records of customers and conduct review under circumstances of certain triggering events, including:

(a) when a significant transaction (i.e. in terms of monetary value or where the transaction is unusual or not in line with the licensee's knowledge of the customer) is to take place;
(b) when a material change occurs in the way the customer's account is operated;
(c) when GRDA's customer documentation standards change substantially; or
(d) when GRDA is aware that it lacks sufficient information about the customer concerned.

All high-risk customers should be subject to a minimum of an annual review, and more frequently if deemed necessary by GRDA, of their profile to ensure the CDD information retained remains up-to-date and relevant.

SIMPLIFIED DUE DILIGENCE (SDD)

Where SDD applies, GRDA is not required to identify and verify the BENEFICIAL OWNER. However, other aspects of CDD must be undertaken and it is still necessary to conduct ongoing monitoring of the business relationship. GRDA must have solid grounds to support the use of SDD and may have to demonstrate these grounds to the Registrar.

To whom may SDD be applied?

Pursuant to section 4(3) of Part 2 of Schedule 2 to the AMLO, customers to whom SDD may be applied are:

(a) financial institution;
(b) an institution that :
  i. is incorporated or established in an equivalent jurisdiction;
  ii. carries on a business similar to that carried on by a financial institution;
  iii. has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and
  iv. is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the regulatory authorities;
(c) a corporation listed on any stock exchange;
(d) an investment vehicle where the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle is -
  i. a financial institution;
  ii. an institution incorporated or established in Hong Kong, or in an equivalent jurisdiction that-
    1) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and
    2) is supervised for compliance with those requirements.
(e) the Government or any public body in Hong Kong; or
(f) the government of an equivalent jurisdiction or a body in an equivalent jurisdiction that performs functions similar to those of a public body.

What customer information GRDA needs under SDD?

GRDA is required to :

(a) identify the customer and verify the customer's identity;
(b) if a business relationship is to be established and its purpose and intended nature are not obvious, obtain information on the purpose and intended nature of the business relationship with GRDA; and
(c) if a person purports to act on behalf of the customer,
  i. identify the person and take reasonable measures to verify the person's identity; and
  ii. verify the person's authority to act on behalf of the customer.

How to ascertain whether SDD is applicable ?

To ascertain whether a customer is eligible for SDD, GRDA would:

(a) verify that the customer is a financial institution or institution on the list of authorised (or supervised) financial institutions in the jurisdiction concerned;
(b) obtain proof of listed status on a stock exchange; or
(c) ascertain that the person responsible for carrying out measures that are similar to the CDD measures in relation to all the investors of the investment vehicle falls within any of the categories of institution set out in section 4(3)(d) of Part 2 of Schedule 2 to the AMLO.

ENHANCED DUE DILIGENCE (EDD)

Section 15 of Part 2 of Schedule 2 to the AMLO specifies that a TCSP licensee must take additional measures or EDD to mitigate the risk of ML/TF in any situation that by its nature presents a higher risk of ML/TF.

High-risk situations for which EDD apply

(a) customer not physically present for identification purposes
(b) customer or its beneficial owner being a politically exposed person
(c) corporate customer which has issued bearer shares
(d) customer from or transaction connected with a jurisdiction that does not adopt or insufficiently adopts the FATF recommendations; and
(e) any situation specified by the Registrar in a notice given to GRDA.

Customer not physically present

If a customer has not been physically present for identification purposes, GRDA must carry out at least one of the following measures to mitigate the risk posed:

(a) further verifying the customer's identity on the basis of documents, data or information not previously used for the purposes of verification of the customer's identity;
(b) taking supplementary measures to verify information relating to the customer that has been obtained by GRDA;
(c) ensuring that the first payment made into the customer's account is received from an account in the customer's name with an authorised institution or a bank operating in an equivalent jurisdiction that has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2 to the AMLO and is supervised for compliance with those requirements by a banking regulator in that jurisdiction.

Politically exposed person (PEP)

Being a PEP does not itself automatically mean that a person is corrupt or has been incriminated in any corruption. However, the office and position may render a PEP vulnerable to corruption. The risk increases when the PEPis from a foreign country with widely-known problems of bribery, corruption and financial irregularity within their government and society. This risk is even more acute where such countries do not have adequate AML/CTF standards.

When GRDA knows that a particular customer or beneficial owner is a PEP (domestic or non-domestic), d, before establishing a business relationship or continuing an existing business relationship where the customer or the beneficial owner is subsequently found to be a PEP, GRDA should apply all the following EDD measures:

(a) obtaining approval from its senior management;
(b) taking reasonable measures to establish the customer's or the beneficial owner's source of wealth and the source of the funds; and
(c) applying enhanced monitoring to the relationship in accordance with the assessed risk.

Corporate customer which has issued bearer shares

GRDA should not onboard the customer.

Customer from urisdiction that does not adopt or insufficiently adopts the FATF Recommendations

GRDA should not onboard the customer.