General Reserve of Digital Assets Limited

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICIES, PROCEDURES AND CONTROLS

“GRDA APPC”

Updated : 30 June 2024

CONTENTS

CHAPTER 1
INTRODUCTION

1.1 All employees of General Reserve of Digital Assets Limited (“GRDA”) are required to comply with the policies and procedures set out in this Anti-Money Laundering and Counter Terrorist Financing Policies, Procedures and Controls (the “APPC”). 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”) and the Guideline on Compliance of Anti-Money Laundering and Counter-Terrorist Financing Requirements for Trust or Company Service Providers (the “Guideline”). Together the AMLO and the Guideline form the rules and regulations (the “Regulation”) for which GRDA business is carried out.

1.2 The key principles for this APPC are:

(a) *Principle 1—responsibilities.* The board of directors of GRDA is responsible for approving the policies, procedures, systems and controls necessary to ensure the effective prevention of money laundering and terrorism financing. The senior management of the firm must ensure that the policies, procedures, systems and controls are implemented, and that they appropriately and adequately address the requirements of the Regulations.

(b) *Principle 2—risk-based approach.* GRDA must adopt a risk-based approach to these policies and their requirements.

(c) *Principle 3—know your customer.* GRDA must know each of its customers to the extent appropriate for the customer’ s risk profile.

(d) *Principle 4—effective reporting.* GRDA must have effective measures in place to ensure that there is internal and external reporting whenever money laundering or terrorism financing is known or suspected.

(e) *Principle 5—high standard screening and appropriate training.* GRDA must:
   i. have adequate screening procedures to ensure high standards when appointing or employing officers and employees; and
   ii. have an appropriate ongoing Regulation training programme for its officers and employees

(f) *Principle 6—evidence of compliance*. GRDA must be able to provide documentary evidence of its compliance with the requirements of the Regulation.

1.3 List of abbreviations :

CDD	Customer Due Diligence
CR	Companies Registry
DTROPO	Drug Trafficking (Recovery of Proceeds) Ordinance (Cap.405)
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
JFIU	Joint Financial Intelligence Unit
KYC	Know Your Customer
OSCO	Organized and Serious Crimes Ordinance (Cap. 455)
TCSP	Trust or Company Service Provider
UNATMO	United Nations (Anti-Terrorism Measures) Ordinance (Cap.575)
UNSO	United Nations Sanctions Ordinance (Cap. 537)

CHAPTER 2
SENIOR MANAGEMENT OVERSIGHT

2.1 Senior management of GRDA should be satisfied that GRDA's Anti-Money Laundering ("AML")/Counter Terrorist Financing ("CTF") systems are capable of addressing its money laundering ("ML") / terrorist financing ("TF") risks.

2.2 Senior management shall appoint a director or senior manager as a Compliance Officer ("CO") who has overall responsibility for the establishment and maintenance of GRDA's AML/CFT systems.

2.3 Senior management shall appoint a senior staff as GRDA's Money Laundering Reporting Officer ("MLRO") who is the central reference point for suspicious transaction reporting.

2.4 The duties and responsibilities of CO include but not limited to:

(a) responsible for all regulatory compliance, KYC, CDD, AML and CTF matters;
(b) develop and review GRDA's AML/CFT systems to ensure they remain up-to-date and meet current statutory and regulatory requirements;
(c) oversight of all aspects of GRDA's AML/CFT systems which include monitoring effectiveness and enhancing the controls and procedures where necessary;
(d) responsible for TCSP compliance;
(e) assist MLRO in carrying out MLRO's duties and responsibilities.

2.5 The duties and responsibilities of MLRO include but not limited to:

(a) assist senior management to set up anti-money laundering policies;
(b) assist senior management to approve and audit customer and transaction information;
(c) assist senior management to monitor customers and analyze transactions on an ongoing basis;
(d) report and alert senior management on money laundering activities;
(e) review all internal disclosures and exception reports and, in light of all available relevant information, determining whether or not it is necessary to make a report to the JFIU;
(f) maintain all records related to such internal reviews;
(g) providing guidance on how to avoid "tipping off" if any disclosure is made;
(h) act as the main point of contact with the JFIU, law enforcement, and any other competent authorities in relation to ML/TF prevention and detection, investigation or compliance;
(i) assist senior management on staff training.

CHAPTER 3
RISK ASSESSMENT AND CUSTOMER ACCEPTANCE

3.1 Compliance Department should assess the ML/TF risks of GRDA's clients by assigning a ML/TF risk rating to each client.

3.2 It should also record its work done on a Risk Assessment Form to demonstrate:

(a) how the client's ML/TF risk is assessed; and
(b) the extent of CDD and ongoing monitoring that is appropriate for the client.

3.3 Relevant factors to be considered by Compliance in the assessment process include the following:

(a) *Country Risk.* Whether the client resides in or is connected with high-risk jurisdictions for example:
   i. those that have been identified by the FATF as jurisdictions with strategic AML/CFT deficiencies (e.g. Iran, the Democratic People's Republic of Korea ("DPRK"), etc);
   ii. countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations (e.g. Afghanistan, Sudan, etc);
   iii. countries which are vulnerable to corruption (e.g. DPRK, the Philippines, etc); or
   iv. those countries that are believed to have strong links to terrorist activities (e.g. Iraq, Afghanistan, etc).

(b) *Customer Risk.* Where the client is of such a legal form that enables individuals to divest themselves of ownership of property whilst retaining an element of control over it or the business/ industrial sector to which a client has business connections is more vulnerable to corruption.

The following types of clients, by their nature or behavior, might also present a higher risk of ML/TF:
   i. Politically Exposed Persons ("PEPs") and/or any individuals connected with them.
   ii. corporate clients that use complex corporate structures, trusts or use nominee and bearer shares where there is no legitimate commercial rationale to do so;
   iii. clients who request to use numbered accounts or undue levels of secrecy with a transaction;
   iv. clients who are involved in cash-intensive businesses (e.g. casinos, money-changers, etc);
   v. clients whose origin of wealth or ownership cannot be reasonably verified.

(c) *Product / Service Risk.* The characteristics of the products and services that GRDA offers and the extent to which they are vulnerable to ML/TF abuse should be considered.

The risks of new products/ services (especially those that may lead to misuse of technological developments or facilitate anonymity in ML/TF schemes) should therefore be assessed before they are introduced to clients. Appropriate additional measures and controls should also be implemented to mitigate and manage their associated ML/TF risks.

(d) *Delivery / Distribution Channel Risk.* The delivery/distribution channels (including business through internet, postal or telephone channels where a non-face-to-face account opening approach is used) and the extent to which the products and services that GRDA offers are vulnerable to ML/TF abuse should be considered. Business referred by intermediaries may also increase risk as the business relationships between the clients and GRDA become indirect.

3.4 Senior management approval is required for opening of accounts for clients associated with risky attributes.

3.5 No business relationship can be established or continued with a client ascertained to be of absolute risk of money laundering and/or terrorist financing and appear on a published list of money launderers/ suspected terrorists.

3.6 Compliance Departments are responsible for conducting AML checks on account applicants and related parties (e.g. beneficiary owners) before opening a customer account.

3.7 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.

3.8 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.

3.9 While carrying out due diligence it would be ensured that there is no harassment to the customer. 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.

3.10 Any existing account where GRDA is not able to apply appropriate CDD 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.

3.11 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.

3.12 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.

3.13 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.

3.14 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 in Appendix E, which would be reviewed periodically by the Independent Audit of GRDA.

CHAPTER 4
CUSTOMER DUE DILIGENCE (“CDD”)

4.1 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”).

4.2 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.

4.3 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 (b) 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.

4.4 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.

4.5 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.

4.6 GRDA should verify the customer's identity by reference to documents, data or information provided by:

(a) a governmental body;
(b) the CR or any other regulatory authority;
(c) an authority in a place outside Hong Kong that performs functions similar to those of the CR or any other regulatory authority;
(d) a digital identification system that is a reliable and independent source that is recognized by the CR; or
(e) any other reliable and independent source that is recognized by the CR.

4.7 GRDA shall conduct the customer name scan and background screening on:

(a) internet;
(b) SentroWeb-DJ;
(c) Accuity.

4.8 Identification and verification of different types of customers are set out in Appendix A to D of this APPC.

4.9 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 CR. 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; or
   ii. an institution that:
      a) incorporated or established in Hong Kong or in an equivalent jurisdiction;
      b) has measures in place to ensure compliance with requirements similar to those imposed under Schedule 2; and
      c) 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.

4.10 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.

4.11 For 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 easonable measures to verify the person’ s identity; and
   ii. verify the person’ s authority to act on behalf of the customer.

4.12 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 PEP;
(c) corporate customer which has issued bearer shares;
(d) customer from or transaction connected with a jurisdiction identified by the FATF as having strategic AML/CTF deficiencies; and
(e) any situation specified by the CR in a notice given to TCSP licensee.

4.13 GRDA should not accept customer in the high-risk situtaion of 4.12(b)(c)(d)(e).

4.14 If a customer has not been physically present for identification purposes, and the identity of the customer can not be verified by a digital identification system that is a reliable and independent source that is recognized by the CR as stated in paragraph 4.6, 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.

4.15 The definitions of different types of PEPs are set out as follows:

(1) A *non-Hong Kong PEP* is defined as:
  (a) an individual who is or has been entrusted with a prominent public function in a place outside Hong Kong and
    i. includes a head of state, head of government, senior politician, senior government, judicial or military official, senior executive of a state-owned corporation and an important political party official;
    ii. but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph a) above;
  (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
  (c) a close associate of an individual falling within paragraph (a) above (see paragraph (3) below).

(2) A *former non-Hong Kong PEP* is defined as:
  (a) an individual who, being a non-Hong Kong PEP, has been but is not currently entrusted with a prominent public function in a place outside Hong Kong;
  (b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or
  (c) a close associate of an individual falling within paragraph (a) above (see paragraph (3) below).

(3) A *close associate* is defined as:
  (a) an individual who has close business relations with a person falling under paragraph 1(a) above, including an individual who is a beneficial owner of a legal

person or trust of which the person falling under paragraph 1(a) is also a beneficial owner; or

(b) an individual who is the beneficial owner of a legal person or trust that is set up for the benefit of a person falling under paragraph 1(a).

(4) A *Hong Kong PEP* means:

(a) an individual who is or has been entrusted with a prominent public function in Hong Kong and

i. includes head of government, senior politician, senior government or judicial official, senior executive of a government-owned corporation and an important political party official;

ii. but does not include a middle-ranking or more junior official of any of the categories mentioned in subparagraph (i) above;

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a) above (see paragraph (3) above).

(5) An *international organisation PEP* means:

(a) an individual who is or has been entrusted with a prominent function by an international organisation, and

i. includes members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions;

ii. but does not include a middle-ranking or more junior official of the international organisation;

(b) a spouse, a partner, a child or a parent of an individual falling within paragraph (a) above, or a spouse or a partner of a child of such an individual; or

(c) a close associate of an individual falling within paragraph (a) above (see paragraph (3) above).

International organisations referred to in paragraph E above are entities established by formal political agreements between their member States that have the status of international treaties; their existence is recognised by law in their member countries; and they are not treated as resident institutional units of the countries in which they are located. Examples of international organisations include the United Nations and affiliated international organisations such as the International Maritime Organisation; regional international organisations such as the Council of Europe, institutions of the European Union, the Organisation for Security and Co-operation in Europe and the Organisation of American States; military international organisations such as the North Atlantic Treaty Organisation, and economic organisations such as the World Trade Organisation or the Association of Southeast Asian Nations, etc.

CHAPTER 5
ONGOING MONITORING OF BUSINESS RELATIONSHIP WITH CUSTOMERS

5.1 In order to help GRDA to update its knowledge of the customers and detect unusual or suspicious activities, GRDA must continuously monitor the business relationship with a customer by:

(a) reviewing from time to time documents, data and information relating to the customer that have been obtained for the purpose of complying with CDD requirements to ensure that they are up-to-date and relevant;
(b) conducting appropriate scrutiny of transactions carried out for the customer to ensure that they are consistent with the licensee's knowledgeof the customer and the customers' business, risk profile and source of funds; and
(c) identifying transactions that are complex, unusually large in amount or of an unusual pattern or that have no apparent economic or lawful purpose and which may indicate ML/TF.

5.2 Transactional monitoring should be performed at the time of each transaction.

5.3 The procedures of transactional monitoring are:

(a) identifying unusual customer transactions. The aspects should be considered are:
    i. the nature and type of individual transactions;
    ii. the nature of a series of transactions;
    iii. the amount of the transactions, paying special attention to particularly substantial transactions;
    iv. the geographical origin/destination of a payment or receipt; and
    v. the customer's usual pattern of activities or turnover.
(b) examination of the background and purposes of transactions;
    i. examinations or enquiries may include asking the customer appropriate questions;
    ii. such enquiries, when conducted properly and in good faith, will not constitute tipping-off.
    iii. the results of the enquiries should be properly documented and be available for inspection by the CR, other authorities and auditors;
    iv. where there is any suspicion, a STR must be made to the JFIU.

5.4 In case where cash transactions or transfers to third parties are being proposed by a customer and such requests are not in accordance with the customer's known pattern of practice, GRDA must be cautious and make relevant further enquiries. Where GRDA having made the necessary enquiries, does not consider the cash transaction or third party transfer reasonable, it should make a STR to the JFIU.

5.5 Periodic monitoring should be performed:

(a) at least once every 2 years for all active customers;
(b) CDD review for medium risk customers shall be carried out at least once a year;
(c) EDD review for high risk customers shall be carried out at least twice a year;
(d) and/or upon changing of the business relationship which include:
    i. setting up new corporate or trust structures;
    ii. buying new products or services that pose higher risk;
    iii. unusual changes or increase of the activities or turnover of a customer; or
    iv. unusual changes in the nature of transactions of a customer.

5.6 Where the basis of the business relationship changes significantly, GRDA should carry out further CDD procedures to ensure that the ML/TF risks involved and basis of the relationship are fully understood.

CHAPTER 6
SUSPICIOUS TRANSACTION REPORT (“STR")

6.1 Transactions or incidents which are identified/noted by any staff of GRDA as unusual and are suspicious of ML/TF should be escalated to the MLRO. Upon receipt of an internal STR, the MLRO will provide a receipt acknowledgement to the reporter and remind him/her of his/her obligation not to tip-off the client(s) involved.

6.2 The MLRO is responsible to justify whether the transaction/incident provides grounds for knowledge or suspicion of ML/TF, and should file a STR to the JFIU as soon as it is reasonable to do so if the internal STR is justified.

6.3 Under no circumstances should reports raised by any staff be filtered out by supervisors or managers who have no responsibility for the money laundering reporting/ compliance function.

6.4 The law requires the STR to be submitted to the JFIU together with any matter on which the knowledge or suspicion is based. The need for prompt reporting is especially important where a client has instructed GRDA to move funds or other property, close the account, make cash available for collection, or carry out significant changes to the business relationship. In such circumstances, consideration may be given to contact the JFIU urgently.

6.5 Once a staff has reported his/her suspicion to the MLRO, he/she has fully discharged his/her reporting obligation under the AMLO.

6.6 The tipping-off provision includes circumstances where a suspicion has been raised internally, but has not yet been reported to the JFIU. All staff should note that tipping off is a criminal offense since it involves disclosure to any person information which might prejudice an investigation. The maximum penalty for the offence upon conviction is imprisonment for 3 years and a fine.

6.7 However, at times when a Client Service Department/Compliance Department/Senior Management is examining suspicious transactions and need to ask the related client(s) questions which, based on common sense, a reasonable person would ask in the circumstances, such enquires, when conducted properly and in good faith, do not constitute tipping off. However, the enquiries made and the responses obtained from the client(s) should be properly documented and should be available to assist the JFIU, other authorities and auditors.

6.8 Examples of unusual/ suspicious transactions are listed in Appendix G.

CHAPTER 7
RECORD KEEPING AND RETENTION

7.1 Customer, transaction and other records that are necessary and sufficient to meet the record-keeping requirements under the AMLO should be properly maintained, to ensure that:

(a) the audit trail for funds moving through GRDA that relates to any client and, where appropriate, the beneficial owner of the client, account or transaction is clear and complete;
(b) any client and, where appropriate, the beneficial owner of the client can be properly identified and verified;
(c) all client and transaction records and information are available on a timely basis to CR, other authorities and auditors upon request; and
(d) proper records of client risk assessment, registers of suspicious transaction reports (including records of internal and external STRs) and training records are retained.

7.2 Where customer identification and verification documents and records are held by a Specified Intermediary which is not an financial institution (Non-FI), an undertaking should also be obtained from the Non-FI that:

(a) it will supply copies of all underlying CDD information to GRDA in circumstances where it is about to cease trading, or does not act as an intermediary for GRDA anymore;
(b) if GRDA has doubts on the CDD measures previously carried out by the Non-FI, it should perform the required CDD as soon as reasonably practicable.

7.3 Specified Intermediary is defined in the AMLO as:

(a) any of the following persons who is able to satisfy the financial institution that they have adequate procedures in place to prevent money laundering and terrorist financing:
    i. a solicitor practicing in Hong Kong;
    ii. a certified public accountant practicing in Hong Kong;
    iii. a current member of The Hong Kong Institute of Chartered Secretaries practicing in Hong Kong;
    iv. a trust company registered under Part VIII of the Trustee Ordinance (Cap. 29) carrying on trust business in Hong Kong;
(b) a financial institution that is an authorized institution, a licensed corporation, an authorized insurer, an appointed insurance agent or an authorized insurance broker; or
(c) a lawyer, a notary public, an auditor, a professional accountant, a trust or company service provider or a tax advisor practicing in an equivalent jurisdiction, or a trust company carrying on trust business in an equivalent jurisdiction, or an institution that carries on in an equivalent jurisdiction a business similar to that carried on by a financial institution mentioned in paragraph above, that:

i. is required under the law of that jurisdiction to be registered or licensed or is regulated under the law of that jurisdiction;
ii. has measures in place to ensure compliance with requirements similar to those imposed under this Schedule; and
iii. is supervised for compliance with those requirements by an authority in that jurisdiction that performs functions similar to those of any of the relevant authorities.

7.4 The record-keeping requirements in respect of each customer and each transaction are illustrated in Appendix E.

CHAPTER 8
STAFF SCREENING AND TRAINING

8.1 GRDA staff screening procedures for the appointment or employment of officers and employees must ensure that an individual is not appointed or employed unless:

(a) for a higher-impact staff — GRDA is satisfied that the individual has the appropriate character, knowledge, skills and abilities to act honestly, reasonably and independently; or
(b) for any other individual — GRDA is satisfied about the individual's integrity.

8.2 Higher-impact staff, means a staff who has a role in preventing money laundering or terrorism financing under the GRDA's AML/CFT programme, they include:

(a) a senior manager of GRDA;
(b) GRDA CO and MLRO;
(c) a staff whose role in the firm includes conducting any other activity with or for a customer.

8.3 Before appointing or employing a higher-impact staff, GRDA must:

(a) obtain references about the individual;
(b) obtain information about the individual's employment history and qualifications;
(c) obtain details of any regulatory action taken in relation to the individual;
(d) obtain details of any criminal convictions of the individual; and
(e) take reasonable steps to confirm the accuracy and completeness of information that it has obtained about the individual.

8.4 The hiring supervisor of the vacant position should evaluate applications against the requirements of the post. In preparing relevant selection criteria:

(a) identify the main purpose of the position;
(b) identify the duties or responsibilities which must be performed to achieve this purpose;
(c) determine the indicators of successful performance of these duties;
(d) determine the essential and desirable qualifications, skills, knowledge and experience required.

8.5 All GRDA staff should aware of:

(a) GRDA’ s statutory obligations and their own personal statutory obligations and the possible consequences for failure to report suspicious transactions under the DTROPO, the OSCO and the UNATMO;

(b) any other statutory and regulatory obligations that concern GRDA and themselves under the AMLO, the DTROPO, the OSCO, the UNATMO and the UNSO, and the possible consequences of breaches of these obligations;
(c) GRDA’ s policies and procedures relating to AML/CTF, including suspicious transaction identification and reporting; and
(d) any new and emerging techniques, methods and trends in ML/TF to the extent that such information is needed by the staff to carry out their respective roles with respect to AML/CTF.

8.6 All new staff irrespective of seniority, areas to be covered in training should include, among others:

(a) an introduction to the background of ML/TF and the importance of AML/CTF to GRDA; and
(b) the need and obligation to identify and report suspicious transactions to the MLRO, and the offence of “tipping-off”;
(c) the importance and the application of GRDA Internal Suspicious Transaction Reporting Form (GISTR).

8.7 Front-line staff whom deals with customers directly, areas to be covered in training should include, among others:

(a) the importance of their roles in GRDA’ s AML/CTF strategy being the first point of contact with potential money launderers and persons involved in terrorist financing;
(b) GRDA’ s policies and procedures in relation to CDD and record-keeping requirements relevant to their job responsibilities;
(c) guidance or tips for identifying unusual activities in different circumstances that may give rise to suspicion; and
(d) the relevant policies and procedures for reporting unusual activities, including the line of reporting and the circumstances where extra vigilance might be required.

8.8 Back-office staff whom does not deal with customers directly but involved in the processing of customer information or customer transactions, areas to be covered in training should include, among others:

(a) appropriate training on customer verification and the relevant processing procedures; and
(b) ways to recognise unusual activities including abnormal settlements, payments or delivery instructions.

8.9 Managerial staff including internal audit staff and CO, areas to be covered in training should include, among others:

(a) higher level training covering all aspects of Hong Kong’ s AML/CTF regime;

(b) specific training in the AML/CTF requirements applicable to TCSP licensees; and
(c) specific training in relation to their responsibilities for supervising or managing staff, auditing the system and performing random checks as well as the reporting of suspicious transactions to the JFIU.

8.10 MLRO, areas to be covered in training should include, among others:

(a) specific training in relation to the MLRO's responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the JFIU; and
(b) training to keep abreast of AML/CTF requirements/developments generally.

8.11 GRDA should maintain staff's training records, including the date and type of training received by each staff. Training records of staff should be maintained for a minimum of 3 years and be made available to the CR on demand.

8.12 GRDA must monitor the effectiveness of the training. This will be achieved by:

(a) testing staff's understanding of the GRDAs policies and procedures to combat ML/TF, their understanding of relevant statutory and regulatory obligations, and also their ability to identify suspicious transactions; and
(b) monitoring the compliance of staff with the GRDA's AML/CTF systems as well as the quality and quantity of internal reports so that further training needs may be identified and appropriate action can be taken.

8.13 Performance appraisal systems for staff will be designed to include integrity as a key assessment factor. The level of assessment should be proportionate to their role in the licensee and the ML/TF risks they may encounter.

CHAPTER 9
INDEPENDENT AUDIT FUNCTION

9.1 GRDA must establish an independent audit function to review the effectiveness of its AML/CTF systems. The responsibilities of an independent audit function are:

(a) to review the adequacy of the licensee's AML/CTF systems, money laundering and/or terrorist financing ("ML/TF") risk assessment framework and application of risk-based approach;
(b) to review the effectiveness of suspicious transaction reporting systems;
(c) to review the effectiveness of the compliance function;
(d) to review the level of awareness of staff having AML/CTF responsibilities.

9.2 A member of the board of directors of GRDA whom is not the CO or MLRO shall head the independent audit function.

APPENDIX

APPENDIX A
IDENTIFICATION AND VERIFICATION – INDIVIDUAL

1. Information of customer to be collected include:

   (a) Full name;
   (b) Date of birth;
   (c) Nationality;
   (d) Identity document type and number; and
   (e) Residential address.

2. GRDA is required to obtain the following documents for verification of the information as stated in paragraphs (1)(a) to (d) above and retain a copy of the documents for record keeping:

   (a) Hong Kong residents:
   - Hong Kong identity card for permanent residents;
   - Birth certificate of a minor (i.e. a person who has not attained the age of 18 years) not in possession of a valid travel document or Hong Kong identitycard (the identity of the minor's parent or guardian representing or accompanying the minor should also be recorded and verified); or
   - Travel document (a copy of the "biodata" page should be retained).

   (b) Non-residents:
   - A valid travel document;
   - A relevant national identity card (issued by government) bearing the person's photograph; A valid national driving licence (issued by government) bearing the person'sphotograph; or
   - Where customers do not have a travel document or a national identity card or driving licence with a photograph, GRDA may, exceptionally and applying a risk-based approach, accept other documents as evidence of identity. Wherever possible such documents should have a photograph of the individual.

3. Travel document includes a passport or some other document which contains a photograph of the holder establishing the identity and nationality, domicile or place of permanent residence of the holder.

APPENDIX B
IDENTIFICATION AND VERIFICATION – CORPORATION

1. Information of customer to be collected include:

   (a) Full name of the corporation;
   (b) Date and place of incorporation;
   (c) Registration or incorporation number; and
   (d) Address of registered office in the place of incorporation and business address (where applicable) (*post office box address is not acceptable*).

2. GRDA is required to obtain the following documents for verification of the information as stated in paragraphs 1(a) to (c) above and retain a copy of the documents for record keeping:

   (a) a copy of the certificate of incorporation and a copy of the business registration certificate (where applicable);
   (b) a copy of the company's articles of association which evidence the powers that regulate and bind the company;
   (c) details of the ownership and control structure of the company, e.g. an ownership chart; and
   (d) a list showing all directors of the corporation.

3. GRDA must:

   (a) confirm that the corporation is still registered and has not been dissolved, wound up, suspended or struck off; and
   (b) independently identify and verify the names of the directors and shareholders recorded in the companies registry in the place of incorporation.

4. For a corporation incorporated in Hong Kong, i.e. a company incorporated under the Companies Ordinance, Cap. 622, the information of the company can be verified against the information in the Companies Register maintained by the CR, by obtaining, for example, a company particulars report and image records of documents showing the shareholders of the company.

5. For a corporation incorporated outside Hong Kong, the information of the corporation can be verified against:

   (a) a similar company search enquiry of the registry in the place of incorporation and obtain a company particulars report;
   (b) a certificate of incumbency or equivalent issued by the company's registered agent in the place of incorporation; or

(c) a similar or comparable document to a company search report or a certificate of incumbency certified by a professional third party in the relevant jurisdiction verifying that the information stated in paragraph 3 above, which is contained in the said document, is correct and accurate.

6. GRDA is required to identify and record the identity of all beneficial owners and take reasonable measures to verify the identity of the beneficial owners. For companies with multiple layers in their ownership structures, a TCSP licensee should ensure that it has an understanding of the ownership and control structure of the company. The intermediate layers of the company should be fully identified.

7. Section 1 of Part 1 of Schedule 2 to the AMLO defines a beneficial owner in relation to a corporation as:

(a) an individual who :
   i. owns or controls, directly or ndirectly, including through a trust or bearer share holding, more than 25% of the issued share capital of the corporation;
   ii. is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights at general meetings of the corporation; or
   iii. exercises ultimate control over the management of the corporation; or
(b) if the corporation is acting on behalf of another person, means the other person.

8. Although GRDA is not required to verify the details of the intermediate companies in the ownership structure of a company, however, complex ownership structures (e.g. structures involving multiple layers, different jurisdictions, trusts, etc.) without an obvious commercial purpose pose an increased risk and may require further steps to be taken so that GRDA is satisfied on reasonable grounds as to the identity of the beneficial owners.

APPENDIX C
IDENTIFICATION AND VERIFICATION – PARTNERSHIP OR UNINCORPORATED BODY

1. Information of customer to be collected include:

   (a) Full name of the partnership or the unincorporated body;
   (b) The names of all partners of the partnership or all members of the unincorporated body and the beneficial owners or office bearers of the partnership or the unincorporated body; and
   (c) The business address (*post office box address is not acceptable)*.

2. GRDA is required to verify the information as stated in paragraphs 1(a) and (b) above using evidence obtained from a reliable and independent source.

3. GRDA is also required to take reasonable measures to verify the identity of the beneficial owners of the partnerships or unincorporated bodies.

4. GRDA should obtain the partnership deed (or other evidence in the case of other unincorporated bodies), to satisfy themselves that the partnership or unincorporated body exists, unless an appropriate national register is available for public inspection.

5. In the case of associations, clubs, societies, charities, religious bodies, institutes, mutual and friendly societies, co-operative and provident societies, GRDA is required to satisfy itself as to the legitimate purpose of the organisation, e.g. by inspecting its constitution.

6. Section 1 of Part 1 of Schedule 2 to the AMLO defines a beneficial owner in relation to a partnership as:

   (a) an individual who
      i. is entitled to or controls, directly or indirectly, more than a 25% share of the capital or profits of the partnership;
      ii. is, directly or indirectly, entitled to exercise or control the exercise of more than 25% of the voting rights in the partnership; or
      iii. exercises ultimate control over the management of the partnership; or
   (b) if the partnership is acting on behalf of another person, means the other person.

7. Under section 1 of Part 1 of Schedule 2 to the AMLO, the beneficial owner in relation to an unincorporated body is defined as:

   (a) an individual who ultimately owns or controls the unincorporated body; or
   (b) if the unincorporated body is acting on behalf of another person, means the other person.

APPENDIX D
IDENTIFICATION AND VERIFICATION – TRUST

1. Information of customer to be collected include:

   (a) the name of the trust, if any;
   (b) date of establishment/settlement;
   (c) the jurisdiction whose laws govern the arrangement, as set out in the trust instrument;
   (d) the identification number (if any) granted by any applicable official bodies (e.g. tax identification number or registered charity or non-profit organisation number);
   (e) identification information of trustee(s) – in line with the verification of the identity for individuals or corporations (please refer to Appendix A or B of this APPC);
   (f) identification information of settlor(s) and any protector(s) or enforcers in verification of the identity for individuals or corporations (please refer to Appendix A or B of this APPC); and
   (g) identification information of known beneficiaries (in line with the verification of the identity for individuals (please refer to Appendix A of this APPC)). Known beneficiaries mean those persons or that class of persons who can, from the terms of the trust instrument, be identified as having a reasonable expectation of benefiting from the trust capital or income.

2. GRDA is required to verify the name and date of establishment of a trust and should obtain appropriate evidence to verify the existence, legal form and parties to it, i.e. trustee, settlor, protector, beneficiary, etc. The beneficiaries should be identified as far as possible where defined.

3. Section 1 of Part 1 of Schedule 2 to the AMLO defines a beneficial owner in relation to a trust as:

   (a) a beneficiary or a class of beneficiaries of the trust entitled to a vested interest in the trust property, whether the interest is in possession or in remainder or reversion and whether it is defeasible or not;
   (b) the settlor of the trust;
   (c) the trustee of the trust;
   (d) a protector or enforcer of the trust; or
   (e) an individual who has ultimate control over the trust.

4. Reasonable measures to verify the existence, legal form and parties to a trust, having regard to the ML/TF risks, may include:

   (a) review and retain a copy of the trust instrument;
   (b) by reference to an appropriate register in the relevant country of establishment;
   (c) a written confirmation from a trustee acting in a professional capacity
   (d) a written confirmation from a lawyer who has reviewed the relevant instrument.

APPENDIX E
INDICATIVE RISK CATEGORIZATION

Low Risk (Level 1)	
RL101	Individuals (Other than included in High and Medium Risk categories below)
RL102	Government departments and Government owned Companies, regulatory and statutory bodies
RL103	NOPs / NGOs promoted by United Nations or its agencies
RL104	All other categories of customer not falling under High and Medium Risk classifications.
Medium Risk (Level 2)	
RL201	Non Bank Financial Institution
RL202	Stock brokerage
RL203	Import/ Export
RL204	Gas Station
RL205	Car/ Boat/ Plane Dealership
RL206	Electronics (wholesale)
RL207	Travel agency
RL208	Used car sales
RL209	Telemarketers
RL210	Providers of telecommunications service, internet café, IDD call service, phone cards, phone center.
RL211	Dot-com company or internet business
RL212	Pawnshops
RL213	Auctioneers
RL214	Cash-intensive Businesses such as restaurants, retail shops, parking garages, fast food stores, movie theaters, etc.
RL215	Sole Practitioners or Law firms (small, little known)
RL216	Notaries (small, little known)
RL217	Secretarial (small, little known)
RL218	Accountants (small, little known)
RL219	Venture capital companies

High Risk (Level 3)	
RL301	Individuals and entities in various United Nations Security council Resolutions (UNSCRs) such as UN 1267 etc.
RL302	Individuals and entities in watch lists issued by Interpol and other similar international organizations.
RL303	customers with dubious reputation as per public information available or commercially available watch lists.
RL304	Individuals and entities specifically identified by regulators, and other competent authorities as high-risk.
RL305	customers conducting their business relationship or transaction in unusual circumstances, such as significant and unexplained geographic distance between the institution and the location of the customer, frequent and unexplained movement of accounts to different institutions in various geographic locations etc.
RL306	customers based in countries/jurisdictions or locations that have been identified by the FATF as jurisdictions with strategic AML/CTF deficiencies
	customers based in countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations
	customers based in countries which are vulnerable to corruption
	customers based in countries that are believed to have strong links to terrorist activities
RL307	Politically exposed persons (PEPs) of foreign origin, customers who are close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner
RL308	Non-resident customers and foreign nationals
RL309	Embassies/ Consulates
RL310	Offshore (foreign) corporation/business
RL311	Non face-to-face customers
RL312	High net worth individuals
RL313	Partnership Firms
RL314	Firms with “sleeping partners”
RL315	Companies having close family shareholding or beneficial ownership
RL316	Complex business ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale
RL317	Shell companies which have no physical presence in the country in which it is incorporated. The existence simply of a local agent or low level staff does not constitute physical presence

RL318	Entities with unexplained use of corporate structures, express trusts and nominee shares, and use of bearer shares
	Entities with unexplained delegation of authority by the customer through the use of powers of attorney, mixed boards and/or representative offices;
	Entities with unexplained relationship between the customer's beneficial owners and controllers and account signatories
	Investment Management/Money Management Company/Personal Investment Company
RL319	Accounts for "gatekeepers' such as accountants, lawyers, or other professionals for their customers where the identity of the underlying customer is not disclosed to the financial institution
RL320	customer Accounts managed by professional service providers such as law firms, accountants, agents, brokers, fund managers, trustees, custodians, etc
RL321	Trusts, charities, NGO's/NPOs unregulated clubs and organizations receiving donations (excluding NPOs/NGOs promoted by United Nations or its agencies)
RL322	Money service Business: including seller of: Orders/ Travelers Checks / Money Transmission /Check Cashing / Dealing or Exchange
RL323	Business accepting third party cheque
RL324	Gambling/gaming including "junket operators" arranging gambling tours
RL325	Dealers in high value or precious goods e.g. jewel, gem and precious metals dealers, art and antique dealers and auction houses
RL326	Customers engaged in a business which is associated with higher levels of corruption (e.g. arms manufacturers, dealers and intermediaries)
RL327	Customers engaged in industries that might relate to nuclear proliferation activities or explosives.
RL328	Customers that may appear to be multilevel marketing companies etc.
RL329	Customers dealing in Real Estate / Construction Activities and activities of similar nature, estate agents and real estate brokers

APPENDIX F
RECORD-KEEPING REQUIREMENTS

	CUSTOMER	TRANSACTION
For how long should records be kept ?	Thoughout the continuance of the business relationship with the customer and for a period of **at least 5 years** after the end of the business relationship. Similarly, for occasional transaction involving an amount equal to or above HKD120,000 (or an equivalent amount in any other currency), **at least 5 years** beginning on the date on which the accasional transaction is completed.	**At least 5 years** after the completion of a transaction regardless of whether the business relationship ends during the period.
What records should be kept ?	The orginal or a copy of : ■ the documents, and a record of the data and information ontained in the course of identifying and verifying the identity of ◆ the customer; ◆ beneficial owner of the customer; ◆ the person who purports to act onbehalf of the customer; and ◆ other connected parties to the customer.	The original or a copy of the documents, and a record of the data and information obtained in connection with the transaction, including the following types of information: ■ the identity of the parties to the transaction; ■ the nature and date of the transaction; ■ the type and amount of currency involved;

	The information should include the additional information obtained for the purposes of EDD or ongoing monitoring. ■ the documents, and a record of the data and information, on the purpose and intended nature of the business relationship; and ■ the files relating to the customer's business relationship and business correspondence with the customer and any beneficial owner of the customer.	■ the origin of the funds (if known); ■ the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc; ■ the destination of the funds; ■ the form of instruction and authority; and ■ the type and identifying number of any account involved in the transaction (where applicable).

APPENDIX G
INDICATORS OF SUSPICIOUS TRANSACTIONS

Examples of unusual/ suspicious transactions are:

(a) transactions that have no apparent economic or lawful purpose, or not in line with the staff's knowledge of the client;
(b) transactions that are inconsistent in amount, origin, destination, or type with a client's known, legitimate business or personal activities;
(c) transactions or instructions which have no apparent legitimate purpose and/or appear not to have a commercial rationale;
(d) transactions, instructions or activity that involve apparently unnecessary complexity or which do not constitute the most logical, convenient or secure way to do business;
(e) where the transaction being requested by the client, without reasonable explanation, is out of the ordinary range of services normally requested, or is outside the experience of the financial services business in relation to the particular client;
(f) where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that has previously emerged;
(g) where the client refuses to provide the information requested without reasonable explanation or who otherwise refuses to cooperate with the CDD and/or ongoing monitoring process;
(h) where a client who has entered into a business relationship uses the relationship for a single transaction or for only a very short period without a reasonable explanation;
(i) the extensive use of trusts or offshore structures in circumstances where the client's needs are inconsistent with the use of such services;
(j) transfers to and from high risk jurisdictions without reasonable explanation, which are not consistent with the client's declared business dealings or interests;
(k) unnecessary routing of funds or other property from/to third parties or through third party accounts; and
(l) where a client fails to complete the identification and verification process.