Your Private Broker

Doo Prime

Anti-Money Laundering And Counter-Terrorism Financing Policy

Updated on 20 February 2023

1. INTRODUCTION

1.1 Doo Prime combats against any forms of money laundering, terrorism financing or criminal activities with a strong dedication by strictly complying with the relevant applicable regulatory regulation.

1.2 Our Money Laundering Reporting Officer("Officer") and other compliance executives are employed to implement the appropriate Anti-Money Laundering and Counter-Terrorism Financing ("AML and CTF") policies and procedures. This AML and CTF policy shall cover procedures and processes:

(a) on the client due diligence requirements;

(b) to implement the record-keeping requirements;

(c) on the reporting requirements;

(d) to inform our officers and employees about money laundering and financing of terrorism, of the policies, processes, procedures and systems adopted by us to deal with money laundering and financing of terrorism;

(e) to train our officers and employees to recognise and deal with money laundering and terrorism financing;

(f) to vet the officers and employees of Doo Prime to ensure that they are fit and proper persons to engage in anti-money laundering and counter-terrorism financing related duties;

(g) on the role and responsibility of the Officer;

(h) on the establishment of an independent audit function which can test its AML and CTF processes, procedures and systems; and

(i) on the adoption of systems by us in dealing with money laundering and terrorism financing.

1.3 Doo Prime has established a series of AML procedures and will apply our AML and Know-Your-client ("KYC") procedures in all transactions. We shall take all reasonable measures to ensure that proper protection exists to prevent a contravention of the Applicable Statutes And Regulations in preventing and mitigating Money Laundering and Terrorism Financing ("ML and TF") activities. Compliance with the AML and CTF system has always been our utmost priority to preserve our business reputation in the global financial industry and regulatory authorities.

1.4 We adopt a risk-based approach in the implementations of our AML and CTF systems and for the purpose of detecting ML and TF risks. We shall update our AML and CTF systems and policies at least once annually to take into account new and emerging risks, considering:

(a) the nature and level of money laundering and terrorism financing risk that we may reasonably expect to face in the course of our business;

(b) the nature, size and complexity of our business;

(c) development of new products and new business practices, including new delivery mechanisms; and

(d) use of new or developing technologies for both new and pre-existing products.

2. DEFINITIONS AND INTERPRETATIONS

2.1 The following terms shall carry the following meaning:

(a) "Applicable Statutes And Regulations" means:

(i) statutes, rules or orders of the Relevant Regulatory Authorities;

(ii) statutes, rules or orders of the relevant regulatory authorities in the client's jurisdiction;

(iii) the rules of the relevant financial exchange market; and

(iv) all other applicable laws to this policy (and each as amended from time to time as applicable to this policy).

(b) "Doo Prime" means any one of the following entities, as may be applicable:

(i) Doo Prime Seychelles Limited, Republic of Seychelles. Doo Prime Seychelles Limited is a licensed securities dealer, authorized and regulated by the

(ii) Doo Prime Mauritius Limited, Republic of Mauritius. Doo Prime Mauritius Limited is a licensed investment dealer, authorized and regulated by the Mauritius Financial Services Commission, and the regulatory number is C119023907;

(iii) Doo Prime Vanuatu Limited, Republic of Vanuatu. Doo Prime Vanuatu Limited is a licensed financial dealer, authorized and regulated by the Vanuatu Financial Services Commission, and the regulatory number is 700238.

(c) "Politically exposed person" or "PEP" means an individual who is or has been entrusted with prominent public functions such as the Head of State, the Prime Minister, Ministers, senior politicians, senior government officials, judicial or military officials, senior executive members of state-owned corporations or international organisations and officials of a political part.

(d) "Proceeds of crime" means property derived or realised directly or indirectly from a serious offence, including:

(i) property into which any property derived or realised directly from the offence is later successively converted or transformed; and

(ii) income, capital or other economic gains derived or realised from that property since the offence.

If property that is proceeds of crime (the original proceeds) is intermingled with other property from which it cannot readily be separated, that proportion of the whole represented by the original proceeds is taken to be proceeds of crime.

(e) "Proliferation financing" means the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

(f) "Relevant Regulatory Authorities" means the relevant regulatory authority which may be applicable to Doo Prime's business operation and service providers, including but not limited to the United States Securities and Exchange Commission, the United States Financial Industry Regulatory Authority, the United Kingdom Financial Conduct Authority, the Australian Securities & Investments Commission, the European Securities and Markets Authority, the Seychelles Financial Services Authority, the Mauritius Financial Services Commission, the Vanuatu Financial Services Commission and etc.

(g) "Source of wealth" refers to the origin of an individual's entire body of wealth (i.e. total assets).

(h) "Source of funds" refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and us (e.g. the amounts being invested, deposited, or wired as part of the business relationship).

(j) "Terrorist financing" or "Terrorism financing" means—

(i) the provision or collection, by any means, directly or indirectly, of any property:

(aa) with the intention that the property be used; or

(ab) knowing that the property will be used, in whole or in part, to commit one or more terrorist acts (whether or not the property is so used);

(ii) the making available of any property or financial (or related) services, by any means, directly or indirectly, to or for the benefit of a person knowing that, or being reckless as to whether the person is a terrorist or terrorist associate; or

(iii) the collection of property or solicitation of financial (or related) services, by any means, directly or indirectly, for the benefit of a person knowing that, or being reckless as to whether the person is a terrorist or terrorist associate.

3. MONEY LAUNDERING

3.1 The stages of money laundering are as follows:

(a) Placement - disposal of cash proceeds derived from illegal activities;

(b) Layering - separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the source of the money, subvert the audit trail and provide anonymity; and

(c) Integration - creating the impression of apparent legitimacy to criminally derived wealth. In situations where the layering process succeeds, integration schemes effectively return the laundered proceeds into the general financial system and the proceeds appear to be the result of, or connected to, legitimate business activities.

3.2 Some of the possible signs of money laundering includes, but is not limited to the following:

(a) reluctance by clients to provide information;

(b) incomplete or inconsistent information by clients;

(c) irregular money transfers and transactions;

(d) unexplained third-party investment;

(e) transactions carried by unusually high volume;

(f) source of funds from poorly-regulated sources;

(g) transactions with no apparent legitimate or economic purpose;

(h) transactions which are unnecessarily complex;

(i) client's lifestyle appears in excess of known sources of income;

(j) business structure is unnecessarily complicated;

(k) use of bank accounts without valid reason;

(l) the client appears to be acting as an agent for another entity or individual but is evasive about the identity of another identity;

(m) the client has multiple accounts under a single name or multiple names, with a large number of inter-account transfers;

(n) the client deposit funds followed by a request to withdraw the funds.

4. CLIENT DUE DILIGENCE ("CDD")

4.1. Doo Prime has established a KYC policy to verify the identities of all our clients and to conduct client due diligence ("CDD"). We perform on-going due diligence process to monitor our client's account, service or relationship with each of our clients to identify, mitigate and manage the risk it may reasonably face with its client that might involve money laundering, financing of terrorism or other serious offences.

4.2 We carry out CDD if a person:

(a) opens an account with us;

(b) engages our services; or

(c) enters into a business relationship with us.

4.3 We carry out CDD on:

(a) a person conducting a transaction;

(b) a person on whose behalf a transaction is being conducted; and

(c) a beneficial owner;

if we have reasonable grounds to believe that the person is undertaking a transaction on behalf of another person. We shall verify whether a person is authorised to undertake the transaction concerned on behalf of the other person.

4.4 Furthermore, we carry out CDD on the client:

(a) before establishing a business relationship with the client;

(b) before carrying out for the client or when the client conducts an occasional transaction that involves an amount equal to or exceeding an aggregate value of USD2,000.00 or it's equivalent in foreign currency for a large cash transaction or international currency transfer, whether carried out in a single operation or several operations that appear if we reasonably think they are linked. In determining whether the transactions are linked, we will consider the factors in Clause 9.6 against the timeframe within which the transactions are conducted;

(c) when we are requested by Relevant Regulatory Authorities, payment service providers or service providers to perform appropriate CDD;

(d) when we carry out an electronic currency transfer for the client;

(e) when we suspect that the client is involved in proceeds of crime, financing of terrorism or a serious offence regardless of the levels of transaction of 4.4(b) above;

(f) when we suspect that the client’s source of funds originated form a third party;

(g) when we suspect that the transaction involves proceeds of crime, or may be used for financing terrorism or for committing a serious offence; or

(h) when we have doubts on the veracity or adequacy of the client identification or information it had previously obtained,

(i) when we are performing our regular CDD routine.

4.5 Required document list

4.5.1 If the client is an individual, we shall collect the following information:

(a) the client's full name;

(b) the client's date of birth;

(c) the client's residential address;

(d) the client's occupation;

(e) the client's country(ies) of citizenship;

(f) the client's country(ies) of residence;

(g) the client's occupation or business activities;

(h) the nature and purpose of the client's proposed relationship with us, including:

(i) the purpose of specific transactions; or

(ii) the expected nature and level of transaction behaviour;

(i) authorization of any person purporting to act for or on behalf of the client;

(j) the income or assets available to the client;

(k) the client's source of funds including the origin of funds;

(l) the client's financial position;

(m) the beneficial ownership of the funds used by the client; and

(n) the beneficiaries of the transactions being facilitated by us on behalf of the client including the destination of funds.

4.5.2 If the client is a foreign registered body corporate, we shall collect the following information:

(a) full name of the foreign company;

(b) the country of registration and full registration detail of the client;

(c) the full address of the company's principal place of business and registered address;

(d) the company structure;

(e) name of each company director and secretary;

(f) nature of the business activities conducted by the company;

(g) name and address of beneficial owners of the company and the control structure;

(h) the country in which the company was formed, incorporated or registered;

(i) the provisions regulating the power to bind the client;

(j) the authorization of any person purporting to act for or on behalf of the client, and the identity of the persons; and

(k) the purpose and intended nature of the business relationship with us.

4.6 We strictly prohibit establishing any business relationship with clients with false, fictitious or misleading names, and we shall make a record of if any of our client is using a different name from which the client is commonly known.

4.7 We will consider on a case by case basis any clients that cannot reasonably be expected to produce the standard evidence of identity and will seek to agree on the use of other confirmations of identity so that clients are not unreasonably denied access to the products and services. In the event it is reasonably proved that there is doubt on the identification and verification of the beneficial owners, we may carry out CDD on the senior management officials of the client in accordance with this AML and CTF policy.

5. CLIENT RISK ASSESSMENT ("CRA")

5.1 Doo Prime will perform CRA using the risk-based approach. We assess the risk for each client taking into account specific products, services, clients, entities, number of transactions, volume of transactions, nature of client relationships, geographic locations, the purpose of the account or relationship, the level of assets involved, the size of transactions to be undertaken and the regularity or duration of the business relationship.

5.2 We will not accept high-risk clients that are identified as follows:

- clients with business that handles a large amount of cash or complex unusually large transactions, which could not be verified.
- clients with large one-off transactions, or several transactions carried out by the same account within a short time.
- clients based in or conducting business in or through, a high-risk jurisdiction, or a jurisdiction with known higher levels of corruption, organized crime, weapon or drug production, distribution, stockpiling or acquisition.
- clients falling under the definition of PEP.
- transactions with the source funds that cannot be verified.
- transactions with no apparent economic or legitimate purpose.
- transactions that might favour anonymity.

5.3 We will conduct a client risk assessment at the initial stage of CDD to determine the extent of CDD measures and ongoing monitoring measures to be applied. We subsequently take a risk-based approach and conduct ongoing monitoring of business relationships with clients to manage and mitigate money laundering and terrorism financing risks, and ensure all related information are updated. The client risk assessment framework shall be proportional to the nature and size of Doo Prime's business with clients.

5.4 When we have any reasonable grounds of suspicion, the client will be required to identify and verify the source or destination of the transactions.

5.5 Our steps to conduct the institutional money laundering/terrorism financing risk assessment include:

(a) documenting the risk assessment process which includes the identification and assessment of relevant risks supported by qualitative and quantitative analysis and information obtained from relevant internal and external sources;

(b) considering all the relevant risk factors before determining the level of overall risk, and the appropriate level and type of mitigation to be applied;

(c) obtaining the approval of senior management on the risk assessment results;

(d) having a process by which the risk assessment is kept up-to-date; and

(e) having appropriate mechanisms to provide the risk assessment to the Relevant Regulatory Authorities when required to do so.

6. SIMPLIFIED DUE DILIGENCE ("SDD")

6.1 If Doo Prime has determined that ML and TF risks are low, Doo Prime may adopt a simplified due diligence ("SDD") approach.

6.2 clients to whom SDD may be applied are:

(a) 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) 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 which:

- has measures in place to ensure compliance with requirements similar to those imposed in the Applicable Statutes And Regulations; and
- is supervised for compliance with those requirements.

(e) the government or any public body; 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.

6.3 In cases of SDD, we will:

(a) identify the client and verify the client'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 us; and

(c) if a person purports to act on behalf of the client,

(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 client.

7. ENHANCED DUE DILIGENCE ("EDD")

7.1 If Doo Prime has determined that ML and TF risks are high, Doo Prime shall adopt an enhanced due diligence ("EDD") approach and enhanced ongoing monitoring. Approval from Doo Prime's senior management will be required before engaging or continuing a business relationship and/or transaction with high risks clients.

7.2 High-risk situations for which EDD apply includes:

(a) client risk factor:

(i) business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic difference between us and the client);

(ii) legal persons or legal arrangements that involve a shell vehicle without a clear and legitimate commercial purpose;

(iii) companies that have nominee shareholders or shares in bearer form;

(iv) cash-intensive business;

(v) the ownership structure of the legal person or legal arrangement appears unusual or excessively complex given the nature of the legal person's or legal arrangement's business; or

(vi) the client or the beneficial owner of the client is a PEP or foreign PEP.

(b) product, service, transaction or delivery channel risk factors:

(i) anonymous transactions (which may involve cash); or

(ii) frequent payments received from unknown or non-associated third parties.

(c) country risk factors. We strictly prohibit all dealings, bank transfers and transactions with clients from high risk countries, including but not limited to:

(i) countries or jurisdictions identified by credible sources, such as mutual evaluation or detailed assessment reports, as not having effective AML and CTF systems;

(ii) countries identified by the Financial Action Task Force;

(iii) countries or jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;

(iv) countries or jurisdictions subject to sanctions, embargoes or similar measures issued by, for example, the United Nations; or

(v) countries, jurisdictions or geographical areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operation.

7.3 Doo Prime reserves the right to obtain information from our independent source for enhanced due diligence measures. This includes but is not limited to:

(a) obtaining additional information on the client (e.g. occupation, volume of assets, ownership and control structure, client's or beneficial owner's reputation, information available through public databases, internet, etc.), and updating more regularly the identification data of the client and beneficial owner;

(b) obtaining additional information on the intended nature, purpose and background of the business relationship and transactions;

(c) obtaining information on the source of funds or source of wealth of the client;

(d) obtaining information on the reasons for intended or performed transactions; and/or

(e) requiring the first payment to be carried out through an account in the client's name with a bank subject to similar CDD standards.

7.4 Our EDD entails:

7.4.1 **Increasing the quantity of information obtained for client due diligence purposes**:

(a) About the client's or beneficial owner's identity, or ownership and control structure, to be satisfied that the risk associated with the relationship is well known. This may include obtaining and assessing information about the client's or beneficial owner's reputation and assessing any negative allegations against the client or beneficial owner. Examples include: information about family members and close business partners; information about the client's or beneficial owner's past and present business activities; and adverse media searches;

(b) About the intended nature of the business relationship, to ascertain whether that the nature and purpose of the business relationship is legitimate and to help firms obtain a more complete client risk profile. It includes obtaining information on:

(i) the number, size and frequency of transactions that are likely to pass through the account to be able to spot deviations that may give rise to suspicions, requesting evidence where appropriate;

(ii) the reason the client is looking for a specific product or service, in particular where it is unclear why the client's needs cannot be met better in another way, or in a different jurisdiction;

(iii) the destination of funds;

(iv) the nature of the client's or beneficial owner's business to understand the likely nature of the business relationship better.

7.4.2 **Increasing the quality of information obtained for client due diligence purposes to confirm the client's or beneficial owner's identity including by:**

(a) Requiring the first payment to be carried out through an account verifiable in the client´s name with a bank;

(b) Establishing that the client's source of wealth and source of funds that are used in the business relationship are not the proceeds from criminal activity and that they are consistent with our knowledge of the client and the nature of the business relationship. The sources of funds or wealth may be verified, among others, by reference to income tax returns, copies of audited accounts, payslips, public deeds or independent and credible media reports;

(c) Increasing the frequency of reviews, to be satisfied that we continue to be able to manage the risk associated with the individual business relationship and to help identify any transactions that require further review, including by:

(i) Increasing the frequency of reviews of the business relationship, to ascertain whether the client's risk profile has changed and whether the risk remains manageable;

(ii) Obtaining the approval of the Officer/nominated officer to commence or continue the business relationship to ensure senior management are aware of the risk we are exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;

(iii) Reviewing the business relationship on a more regular basis to ensure any changes to the client's risk profile are identified, assessed and, where necessary, acted upon;

(iv) Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that may give rise to suspicion of money laundering or terrorism financing. This may include establishing the destination of funds or ascertaining the reason for certain transactions;

(d) The Officer will need to provide approval, or refusal, to proceed with the client set up process before conducting any business with a client who has been through the enhanced due diligence process.

7.5 We will apply EDD measures on any situations, clients or transactions that are deemed to be high risk by us.

7.6 **Source of Funds and Source of Wealth**

7.6.1 Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets).

7.6.2. Source of funds refers to the origin of the particular funds or other assets which are the subject of the business relationship between an individual and us (e.g. the amounts being invested, deposited, or wired as part of the business relationship).

7.7 **How Source of Funds and Source of Wealth measures are incorporated into our EDD Process**

7.7.1 Source of wealth will usually indicate the size of wealth the client would be expected to have, and a picture of how the individual acquired such wealth. Although we may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.

7.7.2 Source of funds information should not simply be limited to knowing from which the funds may have been transferred, but also the activity that generates the funds. The information obtained should be substantive and establish a provenance or reason for the funds having been acquired.

7.8 It is Doo Prime's policy not to accept any funding from any third party, but in the event such exceptional circumstances occur, we shall conduct EDD to identify and verify its ultimate beneficial owner including legal person, partnership, trust and other legal arrangements.

8. VERIFICATION

8.1 We shall verify and screen the client's information above through our client service and risk management department before we establish relationship with them. Our scope of CDD includes, but is not limited to our retail clients, business partners, the board members, shareholders and ultimate beneficial owner. We carry out the following CDD measures:

(a) identify, verify and screen the client's identity and information via an independent screening system;

(b) where there is a beneficial owner in relation to the client, identifying and taking reasonable measures to verify the beneficial owner's identity so that we are satisfied that we know who the beneficial owner is, including in the case where the client is a legal person or trust, measures to enable us to understand the ownership and control structure of the legal person or trust;

(c) obtaining information on the purpose and intended nature of the business relationship (if any) established with us unless the purpose and intended nature are obvious; and

(d) if a person purports to act on behalf of the client:

(i) identifying the person and taking reasonable measures to verify the person's identity using documents, data or information provided by reliable and independent source; and

(ii) verifying the person's authority to act on behalf of the client;

(e) if we deem the identity verification insufficient or if we require additional details relevant to the transaction performed by the client, we reserve the right to request additional details from the client (including but not limited to bank statement, proof of bank account, electronic wallet or electronic currency statement) and reserve our right not to establish a business partnership or proceed with any further transaction. If the client either refuses to provide the required information, or provide false/misleading information, we may freeze the client account, restrict trading or account activity, terminate the business partnership and/or report to the regulatory authority. Upon satisfactory verification of the client's identity and the transaction details, all restrictions applied on the account shall be lifted.

8.2 In the identity verification process, we will request a copy of the original and a coloured scanned copy of the identification documents; we may also request more than one identity documents for cross-verification if we deem necessary.

8.3 When electronic verification is used or a client has not been physically present for identification purposes, we will carry out an additional verification check to manage the risk of impersonation fraud. This check may take the form of:

(a) requiring the first payment to be carried out through an account in the client's name with a regulated credit institution;

(b) telephone contact with the client on a home or business number that has been verified, before opening the account;

(c) communicating with the client at the address that has been verified;

(d) requiring copy documents to be certified by an appropriate person.

8.4 If we are unable to carry out the prescribed identification process on a person, we:

(a) shall not open an account for the person;

(b) shall not enter into a business relationship with the person; and

(c) if a business relationship already exists with the person, we shall terminate the existing business relationship.

9. REPORT

9.1 If satisfactory evidence of the identity or verification of a person is not produced to or obtained by us within 14 working days (2 working days if Clause 4.4(d) and (e) arise), we shall submit a suspicious activity report to the Relevant Regulatory Authorities. We shall not proceed any further with the transaction unless directed to do so by the Relevant Regulatory Authorities.

9.2 In the event we suspect on reasonable grounds that the client is not the person that he or she claims to be, we shall take one or more of the actions below within 3 working days commencing after the day on which the circumstance comes into existence:

(i) collect the necessary client identification information in respect of the client; or

(ii) verify, from a reliable and independent source, certain client information that has been obtained in respect of the client; to ensure it is reasonably satisfied that the client is the person that he or she claims to be.

9.3 When determining and putting in place appropriate risk-based systems and controls, we shall consider the nature, size and complexity of the client's business and type of ML and TF risks that we might reasonably face, including but not limited to the following factors:

(a) client types, including PEPs;

(b) the types of designated services provided;

(c) method by which we deliver designated services, including any development of new products, business practices and use of new or developing technologies;

(d) the foreign jurisdictions with which we deal, including high risk jurisdictions as identified by Financial Action Task Force.

9.4 If any of the following events occurs:

(a) suspicious transaction;

(b) suspicious activity;

(c) transaction conducted by money laundering entities;

(d) transaction involving terrorist property;

(e) transaction with no legitimate purpose;

(f) our supervisory body or auditor has reasonable grounds to suspect that a transaction or an attempted transaction or information that it has in its possession involves proceeds of crime or is related to the financing of terrorism; or

(g) any transaction described in Clause 3.2;

the transaction should be suspended and should not proceed without the authorization of the Officer. Our frontline staff shall report any suspicious transaction or activity without delay to the Officer, who will then make a suspicious activity or suspicious transaction report to the Relevant Regulatory Authorities in 2 working days if required.

9.5 If suspicious signals of money laundering are identified, the transaction should be suspended and should not proceed without the authorization of the Officer. After making appropriate investigations, the Officer will report the matter to the Relevant Regulatory Authorities if we believe there is any potential serious ML and TF risks. In the event we deem a person conducts 2 or more transactions with the intention to avoid the amount threshold as described in Clause 4.4(b), we shall submit a suspicious transaction report to the Relevant Regulatory Authorities. We shall consider the following factors before submitting our report:

(a) the manner and form in which the transactions were conducted;

(b) the amount of the currency involved in each transaction;

(c) the aggregate amount of the currency involved in the transactions;

(d) the period over which the transactions occurred;

(e) the interval of time between the transactions;

(f) the locations at which the transactions were initiated or conducted;

(g) any explanation made by the person concerned as to the manner or form in which the transactions were conducted.

9.6 **Procedure of handling suspicious activity report and suspicious transaction report**

9.6.1 After making appropriate investigations, the Officer will consider, if appropriate, reporting the matter to the regulatory authority. All records to the Officer and the relevant authorities, shall be kept by the Officer for a term of no less than 7 years after the matter has been closed by the regulatory authority. The suspicious activity report or suspicious transaction report shall include:

(a) personal particulars and contact details of the individuals or entities involved in the suspicious activity or transaction;

(b) details of the suspicious activity or transaction;

(c) the suspicious activity or transaction indicators observed; and

(d) any explanation provided by the subject of the suspicious activity report or suspicious transaction report when questioned about the transaction or activity.

9.6.2 The filing of a suspicious activity report or suspicious transaction report to the Relevant Regulatory Authorities provides us a statutory defence to the offence of ML and TF in respect of the acts disclosed in the report, provided that:

(a) the suspicious activity report or suspicious transaction report is made before we undertake the disclosed acts and the acts or transactions are undertaken with the consent of the Relevant Regulatory Authorities; or

(b) the suspicious activity report or suspicious transaction report is made after we have performed the disclosed acts or transactions and the report is made on our initiative and as soon as it is reasonable for us to do so.

9.7 All notifications made will be handled with strict confidentiality. However, please note that there may be circumstances in which we are required to reveal an individual's identity, for example where we are compelled to do so by law and therefore anonymity cannot be guaranteed.

9.8 We are aware that it is an offence for a person, knowing or suspecting that a disclosure has been made to the Relevant Regulatory Authorities, if he/she discloses to any other person any matter which is likely to prejudice any investigation which might be conducted following the disclosure (commonly referred to as "tipping-off"). The client's awareness of a possible suspicious activity report or suspicious transaction report or investigation could prejudice future efforts to investigate the suspected ML and TF operation. Therefore, if we form a suspicion that transactions related to ML and TF, we will take into account the risk of tipping-off when performing the CDD process. We shall ensure that our employees are aware of and sensitive to these issues when conducting CDD.

9.9 We shall not disclose any information to any other person:

(a) that we, or our supervisory body or auditor or a person has formed a suspicion in relation to a transaction or an attempted transaction, or an activity or attempted activity; or

(b) that a report under Applicable Statutes And Regulations is made to Relevant Regulatory Authorities; or

(c) that information under the Applicable Statutes And Regulations is given to Relevant Regulatory Authorities; or

(d) any other information from which a person to whom the information is disclosed may reasonably be expected to infer any circumstances in paragraph (a)-(c).

9.10 Clause 9.9 does not apply to a disclosure made to:

(a) an officer, employee or agent of a Doo Prime who has made or is required to make a report or provide information under this Applicable Statutes And Regulations for any purpose connected with the performance of that our duties; or

(b) a lawyer for the purpose of obtaining legal advice or representation in relation to the disclosure; or

(c) the supervisor of Doo Prime; or

(d) a law enforcement agency or any other person assisting the Relevant Regulatory Authorities under this Applicable Statutes And Regulations.

9.11 The responsibilities of our Officer include, but is not limited to the following:

(a) Review all internal reports of suspicious transactions and exception reports and, in the light of all available information, determine whether or not it is necessary to file a suspicious activity report or suspicious transaction report with the Relevant Regulatory Authorities;

(b) Maintain all records relating to such internal reviews;

(c) Guide staff on how to avoid “tipping-off” if any suspicious activity report or suspicious transaction report is filed;

(d) Applicable Statutes And Regulations as the main point of contact with the Relevant Regulatory Authorities, law enforcement agencies, and any other competent authorities in relation to ML and TF prevention and detection, investigation or compliance.

10. ONGOING CDD AND TRANSACTION MONITORING

10.1 We shall conduct ongoing monitoring through ongoing CDD and transaction monitoring to ensure compliance with the AML and CTF Systems. We shall review the existing CDD records upon any trigger events and maintain adequate systems to monitor transactions in accordance with the risk-based approach adopted. The extent of monitoring shall be proportional to the ML and TF risk profile of a client.

10.2 Ongoing CDD

10.2.1 We continuously monitor the activity of our clients by:

(a) reviewing from time to time documents, data and information relating to the client that have been obtained to comply with CDD requirements to ensure that they are up-to-date and relevant;

(b) conducting appropriate scrutiny of transactions carried out for the client to ensure that they are consistent with our knowledge of the client and the clients’ 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 and TF.

10.2.2 All clients that present:

(a) high ML and TF risks should be subject to a review every 6 months;

(b) medium ML and TF risks should be subject to a review once annually;

(c) low ML and TF risks should be subject to a review once every 2 years;

or more frequent reviews if deemed necessary by us, to ensure the CDD information retained is consistent with our knowledge of the client, the client's business, source of funds and risk profile.

10.2.3 All clients, who have been classed as high risk, will undergo a complete review. This will entail establishing the following:

- Re-confirmation of address
- Re-confirmation of corporate structure (if applicable)
- Re-confirmation of Source of Funds and Wealth
- Screening for adverse news
- Complete review of transaction profile, including new products requested

10.3 Transaction monitoring

10.3.1 We maintain adequate systems to monitor and review all transactions performed based on a risk-based approach, and we shall check and review whether the transactions are normal based on the following factors:

(a) the size and complexity of its business;

(b) the ML and TF risks arising from its business;

(c) the nature of its systems and controls;

(d) the monitoring procedures that already exist to satisfy other business needs; and

(e) the nature of the products and services provided (which includes the means of delivery or communication).

10.3.2 We regularly review the adequacy and effectiveness of its transaction monitoring systems and processes, including parameters and thresholds adopted. The parameters and thresholds adopted include the following factors:

(a) the nature and type of transactions (e.g. abnormal size or frequency);

(b) the nature of a series of transactions (e.g. structuring a single transaction into several cash deposits);

(c) the counterparties of transactions;

(d) the geographical origin/destination of a payment or receipt;

(e) the client's normal account activity or turnover;

(f) the client's behaviour - sudden and/or significant changes in transaction activity by value, volume or nature, such as change in beneficiary or destination;

(g) client's linked relationships – identifying common beneficiaries and remitters amongst apparently unconnected accounts or clients.

11. RECORD KEEPING

11.1 Records of all original and copy of identity verification documents, transaction records, CDD information, ML and TF reports made to Officer, all documents submitted in relation to suspicious activity report, suspicious transaction report, staff handling the suspicious transaction report, results of the suspicious transaction report and other documents necessary under the Officer will be compiled and organized with confidentiality for at least 7 years after the end of the business relationship with clients.

11.2 The record-keeping requirements in respect of each client are as follows:

(a) We must keep the original or a copy of:

(i) the documents, and a record of the data and information obtained in the course of identifying and verifying the identity of the client; beneficial owner of the client; and the person who purports to act on behalf of the client; and

(ii) the files relating to the client's business relationship and business correspondence with the client and any beneficial owner of the client; and

(b) The documents and records mentioned in sub-paragraph (a) above must be kept throughout the continuance of the business relationship with the client and for at least seven years beginning on the date on which the business relationship ends.

11.3 The record keeping requirements in respect of each transaction are as follows:

(a) We will keep the original or a copy of the documents, and a record of the data and information obtained in connection with the transaction, including but not limited to the following:

(i) nature of the transaction;

(ii) the amount of the transaction and the currency in which it was denominated;

(iii) the date on which the transaction was conducted;

(iv) the name, address and occupation, business or principal activity, as the case requires, of each person:

(aa) conducting the transaction; and

(ab) for whom, or for whose ultimate benefit, the transaction is being conducted, if we have reasonable grounds to believe that the person is undertaking the transaction on behalf of any other person;

(v) the type and identifying number of any accounts/services with us that were involved in the transaction;

(vi) if the transaction involves a negotiable instrument other than currency:

(aa) the drawer of the instrument;

(bb) the name of the institution on which it is drawn;

(cc) the name of the payee (if any);

(dd) the amount and date of the instrument; and

(ee) the number (if any) of the instrument and details of any endorsements appearing on the instrument;

(vii) the name and address of Doo Prime, and of each officer, employee or agent of Doo Prime who prepared the relevant record or a part of the record;

(viii) any other information relating to that transaction.

(b) Records required to be kept under subparagraph (a) must be kept for at least seven years beginning on the date on which the transaction is completed, regardless of whether the business relationship ends during the period.

12. AML AND CTF SCREENING PROCESS

12.1 Clients will be screened against lists of sanctions, politically exposed persons, regulatory enforcement, law enforcement, money laundering, terrorism financing, adverse media reports provided by Refinitiv Limited's World-Check One screening system. Clients will be added to World-Check One's ongoing monitoring list whereby their details will be automatically searched by the system every 12 hours. We will receive an alert whenever there are any positive matches.

12.2 We screen:

(a) clients and any beneficial owners of the clients against the current database at the establishment of the relationship;

(b) clients and any beneficial owners of the clients against all new and any updated designations to the database as soon as practicable; and

(c) all relevant parties in a cross-border wire transfer against the current database before executing the transfer.

12.3 In case of any suspicions of terrorism financing, proliferation financing and sanctions violations, we will submit a suspicious activity or suspicious transaction report to the Relevant Regulatory Authorities. We will report any asset frozen or actions taken in compliance with the financial sanctions requirements by way of filing a suspicious activity report or suspicious transaction report to the Relevant Regulatory Authorities.

13. AML AND CTF AUDIT FUNCTION

13.1 The Officer and our compliance department conduct an internal audit on our AML and CTF policy annually to ensure our AML and CTF policy are updated. We are aware of our statutory liability to comply with the Applicable Statutes And Regulations and we shall update and review our AML and CTF policy at least once annually.

13.2 We will regularly identify and assess ML and TF risks that may arise in relation to:

(a) the nature and level of money laundering and terrorism financing risk that we may reasonably expect to face in the course of its business;

(b) the nature, size and complexity of our business;

(c) development of new products and new business practices, including new delivery mechanisms; and

(d) use of new or developing technologies for both new and pre-existing products.

14. TRAINING PROGRAMME

14.1 All relevant staff in Doo Prime will be provided with relevant policy and knowledge training provided in this AML and CTF Policy. In addition, all relevant staff in Doo Prime will be briefed about their job descriptions and will be trained on their responsibilities concerning money laundering and financing of terrorism transactions. They will be guided on how to identify and deal with transactions that possibly involve money laundering and financing of terrorism.

14.2 Scope of training

14.2.1 Staff will be made aware of:

(a) our statutory obligations and their statutory obligations and the possible consequences for failure to report suspicious transactions under the Applicable Statutes And Regulations and the Regulation;

(b) any other statutory and regulatory obligations that concern the us under the Applicable Statutes And Regulations and the Regulation, and the possible consequences of breaches of these obligations;

(c) our policies and procedures relating to AML and CTF, including suspicious activity and transaction identification and reporting;

(d) any new and emerging techniques, methods and trends in ML and TF to the extent that such information is needed by the staff to carry out their respective roles concerning AML and CTF;

(e) escalation procedures, i.e. what to do once a ML and TF risk is identified;

(f) what the employee's role is in our compliance's efforts and how to perform them;

(g) record keeping and record retention policy; and

(h) disciplinary consequences (civil and criminal) for non-compliance with the Applicable Statutes And Regulations.

14.2.2 Focused training for appropriate staff or groups of staff will enable Doo Prime and senior management to implement their AML and CTF systems effectively. The following areas of training may be appropriate for certain groups of staff:

(a) All new staff (irrespective of seniority)

(i) an introduction to the background of ML and TF and the importance of AML and CTF to us; and

(ii) the need and obligation to identify and report suspicious transactions to the Officer, and the offence of "tipping-off".

(b) Front-line staff (i.e. staff dealing with clients directly)

(i) the importance of their roles in the company's AML and CTF strategy being the first point of contact with potential money launderers and persons involved in TF;

(ii) the company's policies and procedures in relation to CDD and record-keeping requirements relevant to their job responsibilities;

(iii) guidance or tips for identifying unusual activities in different circumstances that may give rise to suspicion; and

(iv) the relevant policies and procedures for reporting unusual activities, including the line of reporting and the circumstances where extra vigilance might be required.

(c) Back-office staff

(i) appropriate training on client verification and the relevant processing procedures; and

(ii) ways to recognise unusual activities including abnormal settlements, payments or delivery instructions.

(d) Managerial staff (including internal audit staff)

(i) higher-level training covering all aspects of AML and CTF regime;

(ii) specific training in the AML and CTF requirements applicable to us; and

(iii) 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 Relevant Regulatory Authorities.

(e) Officer

(i) specific training in relation to the Officer's responsibilities for assessing suspicious transaction reports submitted to them and reporting of suspicious transactions to the Relevant Regulatory Authorities;

(iii) training to keep abreast of AML and CTF requirements/developments generally;

(iv) receive reports of suspicious activity from firm personnel; and

(iv) coordinate required AML reviews/meetings with appropriate staff.

14.3 We will monitor the effectiveness of the training. This may be achieved by:

(a) testing staff's understanding of our policies and procedures to combat ML and TF, the understanding of their statutory and regulatory obligations, and also their ability to recognise suspicious transactions;

(b) monitoring the compliance of staff with our AML and 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; and

(c) monitoring attendance and following up with staff who miss such training without reasonable cause.

14.4 We conduct AML training, workshops and assessments on all related staff members at least once annually.

14.5 We shall observe and record our employees who have been adequately trained, when they are trained or last trained, and thereafter provide additional, necessary and adequate training to them.

15. LANGUAGE AND AMENDMENTS

15.1 The official language of this AML and CTF policy shall be English. Doo Prime may provide this AML and CTF policy in other languages for information purposes only and in the event of any inconsistency or discrepancy between the English version of this AML and CTF policy and any other language version, the English version shall prevail.

15.2 The client acknowledges that Doo Prime reserves the right to amend or update this AML and CTF policy at any time without prior notice to the client. The amendments to the AML and CTF policy shall become effective immediately and shall be legally binding on the client upon publishing of the AML and CTF policy on Doo Prime's website. The client undertakes to regularly review this AML and CTF policy on the Doo Prime's website.

(the rest of this page is intentionally left blank)

[中文翻译]

Your Private Broker
Doo Prime

反洗钱和反恐融资政策

2023 年 2 月 20 日更新

1. 介绍

1.1 Doo Prime 严格遵守相关适用的监管规定，以坚定的奉献精神打击任何形式的洗钱、恐怖主义融资或犯罪活动。

1.2 我们的洗钱报告官（“官员”）和其他合规主管负责实施适当的反洗钱和反恐融资（“AML 和 CTF”）政策和程序。 本 AML 和 CTF 政策应涵盖程序和流程：

(a) 根据该适用的法规和条例客户尽职调查要求；

(b) 执行记录保存要求；

(c) 根据报告要求；

(d) 向我们的官员和员工通报有关洗钱和资助恐怖主义的法律，以及我们为处理洗钱和资助恐怖主义而采取的政策、流程、程序和系统；

(e) 培训我们的官员和员工识别和处理洗钱和恐怖主义融资；

(f) 审查 Doo Prime 的官员和员工，以确保他们是从事反洗钱和反恐融资相关职责的合适人选；

(g) 关于该官员的角色和责任；

(h) 关于建立一个独立的审计职能，可以测试其 AML 和 CTF 流程、程序和系统； 和

(i) 关于我们在处理洗钱和恐怖主义融资方面采用的系统。

1.3 Doo Prime 建立了一系列反洗钱程序，并将在所有交易中应用我们的反洗钱和了解您的客户（“KYC”）程序。 我们将采取一切合理措施确保存在适当的保护，以防止在防止和减轻洗钱和恐怖主义融资（“ML 和 TF”）活动中违反适用的法规和条例。 遵守 AML 和 CTF 系统一直是我们维护我们在全球金融行业和监管机构的商业声誉的首要任务。

1.4 我们在实施 AML 和 CTF 系统时采用基于风险的方法，目的是检测 ML 和 TF 风险。 我们将至少每年更新一次我们的 AML 和 CTF 系统和政策，以考虑新出现的风险，同时考虑：

(a) 我们在业务过程中可能合理预期面临的洗钱和恐怖主义融资风险的性质和程度；

(b) 我们业务的性质、规模和复杂性；

(c) 开发新产品和新业务实践，包括新的交付机制； 和

(d) 对新产品和已有产品使用新技术或正在开发的技术。

2. 定义和解释

2.1 以下术语应具有以下含义：

(a) “适用的法规和条例”是指：

(i) 相关监管机构的法规、规则或命令；

(ii) 客户管辖范围内相关监管机构的法规、规则或命令；

(iii) 相关金融交易市场的规则； 和

(iv) 本政策的所有其他适用法律（以及适用于本政策的不时修订的每项法律）。

(b) “Doo Prime”是指以下任何一种实体，如适用：

(i) Doo Prime Seychelles Limited，塞舌尔共和国。Doo Prime Seychelles Limited是一家持牌证券交易商，受塞舌尔金融服务管理局授权和监管，监管编号为SD090；

(ii) Doo Prime Mauritius Limited，毛里求斯共和国。Doo Prime Mauritius Limited是一家持牌投资交易商，受毛里求斯金融服务委员会授权和监管，监管号为C119023907；

(iii) Doo Prime Vanuatu Limited，瓦努阿图共和国。Doo Prime Vanuatu Limited是一家持牌金融交易商，由瓦努阿图金融服务委员会授权和监管， 监管号为700238。

(c) “政治人物”或“PEP”是指被赋予重要公共职能的个人，例如国家元首、总理、部长、高级政治家、高级政府官员、司法或军事官员、高级行政人员 国有企业或国际组织以及政治部门的官员。

(d) “犯罪所得”是指直接或间接从严重犯罪中获得或变现的财产，包括：

(i) 直接从犯罪中获得或变现的任何财产后来依次转换或转化为的财产； 和

(ii) 自犯罪以来从该财产获得或实现的收入、资本或其他经济收益。

如果作为犯罪所得的财产（原所得）与其他不易分离的财产混合在一起，则原所得所代表的全部财产中的该部分被视为犯罪所得。

(e) “扩散融资”是指提供资金或金融服务的行为，这些资金或金融服务全部或部分用于制造、获取、拥有、开发、出口、转运、经纪、运输、转让、储存或使用核 、化学或生物武器及其运载工具和相关材料（包括用于非合法目的的技术和双重用途货物），违反国家法律或适用的国际义务。

(f) “相关监管机构”是指可能适用于 Doo Prime 业务运营和服务提供商的相关监管机构，包括但不限于美国证券交易委员会、美国金融业监管局、英国金融行为监管局 、澳大利亚证券和投资委员会、欧洲证券和市场管理局、塞舌尔金融服务管理局、毛里求斯金融服务委员会、瓦努阿图金融服务委员会等。

(g) “财富来源”是指个人全部财富（即总资产）的来源。

(h) “资金来源”是指个人与我们之间业务关系的标的特定资金或其他资产的来源（例如，作为业务关系的一部分投资、存入或电汇的金额）。

(j) “资助恐怖主义”或是指——

(i) 以任何方式直接或间接提供或收集任何财产：

(aa) 有意图使用该财产； 或

(ab) 知道该财产将全部或部分用于实施一项或多项恐怖行为（无论该财产是否被如此使用）；

(ii) 以任何方式，向明知或罔顾该人是否为恐怖分子或恐怖分子同伙的人直接或间接地为其利益提供任何财产或金融（或相关）服务； 或者

(iii) 以任何方式，向明知或罔顾该人是否为恐怖分子或恐怖分子同伙的人直接或间接收为其集财产或招揽金融（或相关）服务。

3. 洗钱

3.1 洗钱的阶段如下：

(a) 配售 - 处置来自非法活动的现金收益；

(b) 分层——通过创建复杂的金融交易层将非法收益与其来源分开，旨在掩盖资金来源、破坏审计线索并提供匿名性； 和

(c) 整合——给犯罪所得财富创造明显合法性的印象。 在分层过程成功的情况下，整合计划有效地将洗钱收益返回到一般金融系统，并且收益似乎是合法商业活动的结果或与合法商业活动有关。

3.2 一些可能的洗钱迹象包括但不限于以下几点：

(a) 客户不愿提供信息；

(b) 客户提供的信息不完整或不一致；

(c) 不规则的汇款和交易；

(d) 不明原因的第三方投资；

(e) 交易量异常大；

(f) 来自不善监管的资金来源；

(g) 没有明显合法或经济目的的交易；

(h) 不必要地复杂的交易；

(i) 客户的生活方式似乎超出了已知的收入来源；

(j) 业务结构过于复杂；

(k) 无正当理由使用银行账户；

(l) 客户似乎是另一个实体或个人的代理人，但对另一个身份回避；

(m) 客户拥有多个同名或多名账户，账户间转账次数较多；

(n) 客户存入资金，然后请求提取资金。

4. 客户尽职调查（“CDD”）

4.1. Doo Prime 制定了 KYC 政策来验证我们所有客户的身份并进行客户尽职调查（“CDD”）。 我们进行持续的尽职调查，以监控我们的客户账户、服务或与每位客户的关系，以识别、减轻和管理客户可能涉及洗钱、资助恐怖主义或其他严重犯罪的可能面临的风险 .

4.2 我们执行 CDD 如果一个人：

(a) 与我们开户；

(b) 使用我们的服务； 或者

(c) 与我们建立业务关系。

4.3 我们在以下方面进行 CDD：

(a) 进行交易的人；

(b) 代表其进行交易的人； 和

(c) 实益拥有人；

如果我们有合理的理由相信该人正在代表另一个人进行交易。 我们将核实某人是否获授权代表另一人进行有关交易。

4.4 此外，我们对客户端进行 CDD：

(a) 在与客户建立业务关系之前；

(b) 在为客户进行之前或当客户进行偶尔的交易，涉及金额等于或超过 2,000.00 美元或等值外币的大额现金交易或国际货币转账时，无论是在 如果我们合理地认为它们是链接的，则出现的单个操作或多个操作。 在确定交易是否关联时，我们将根据交易进行的时间框架考虑第 9.6 条中的因素；

(c) 当有关监管机构、支付服务提供商或服务提供商要求我们执行适当的 CDD 时；

(d) 当我们为客户进行电子货币转账时；

(e) 当我们怀疑客户涉及犯罪所得、资助恐怖主义或严重犯罪时，无论上述 4.4(b) 的交易水平如何；

(f) 当我们怀疑客户的资金来源来自第三方时；

(g) 当我们怀疑交易涉及犯罪所得，或可能用于资助恐怖主义或犯下严重罪行时； 或

(h) 当我们对之前获得的客户身份或信息的真实性或充分性有疑问时，

(i) 当我们执行常规 CDD 例程时。

4.5 所需文件清单

4.5.1 如果客户是个人，我们将收集以下信息：

(a) 客户的全名；

(b) 客户的出生日期；

(c) 客户的住址；

(d) 客户的职业；

(e) 客户的国籍国；

(f) 客户的居住国；

(g) 客户的职业或商业活动；

(h) 与我们建立业务关系的目的和预期性质，包括：

(i) 特定交易的目的； 或

(ii) 交易行为的预期性质和水平；

(i) 任何声称代表客户或为客户行事的人的授权；

(j) 客户可获得的收入或资产；

(k) 客户的资金来源，包括资金来源；

(l) 客户的财务状况；

(m) 客户使用的资金的实益所有权； 和

(n) 我们代表客户促成的交易的受益人，包括资金的目的地。

4.5.2 如果客户是外国注册法人团体，我们将收集以下信息：

(a) 外国公司的全名；

(b) 客户的注册国家和完整注册详情；

(c) 公司主要营业地点及注册地址的完整地址；

(d) 公司结构；

(e) 每位公司董事和秘书的姓名；

(f) 公司开展的业务活动的性质；

(g) 公司实益拥有人的名称和地址以及控制结构；

(h) 公司成立、注册或注册所在的国家；

(i) 规管约束客户的权力的条文；

(j) 任何声称代表客户或为客户行事的人的授权，以及该人的身份； 和

(k) 与我们建立业务关系的目的和预期性质。

4.6 我们严禁与使用虚假、虚构或误导性名称的客户建立任何业务关系，并且我们将记录我们的任何客户是否使用与客户众所周知的名称不同的名称。

4.7 我们将逐案考虑任何无法合理预期提供标准身份证明的客户，并将寻求同意使用其他身份确认，以便客户不会被无理拒绝访问产品和服务。 如果有合理证据证明受益所有人的身份和核实存在疑问，我们可以根据本《反洗钱和反恐融资政策》对客户的高级管理人员进行 CDD。

5. 客户风险评估（“CRA”）

5.1 Doo Prime 将使用基于风险的方法执行 CRA。 我们评估每个客户的风险，考虑到具体的产品、服务、客户、实体、交易数量、交易量、客户关系的性质、地理位置、账户或关系的目的、所涉及的资产水平、 将进行的交易规模以及业务关系的规律性或持续时间。

5.2 我们将不接受以下认定的高风险客户：

- 无法核实且处理大量现金或复杂异常大笔交易的业务的客户。
- 一次性交易量大的客户，或同一账户在短时间内进行多次交易的客户。
- 客户位于或通过高风险司法管辖区或已知具有较高腐败、有组织犯罪、武器或毒品生产、分销、储存或收购水平的司法管辖区开展业务。
- 客户属于 PEP 的定义。
- 无法核实的来源资金的交易。
- 没有明显经济或合法目的的交易。
- 可能有利于匿名的交易。

5.3 我们将在客户尽职调查的初始阶段进行客户风险评估，以推定客户尽职调查措施的范围和将采用的持续监控措施。 随后，我们采取基于风险的方法，对与客户的业务关系进行持续监控，以管理和减轻洗钱和恐怖主义融资风险，并确保更新所有相关信息。 客户风险评估框架应与 Doo Prime 与客户的业务性质和规模成比例。

5.4 当我们有任何合理的怀疑理由时，客户将被要求识别和验证交易的来源或目的地。

5.5 我们进行机构洗钱/恐怖主义融资风险评估的步骤包括：

(a) 记录风险评估过程，其中包括通过定性和定量分析以及从相关内部和外部来源获得的信息支持的相关风险的识别和评估；

(b) 在确定总体风险水平之前考虑所有相关风险因素，以及要应用的适当缓解水平和类型；

(c) 取得高级管理层对风险评估结果的批准；

(d) 具有使风险评估保持最新的过程； 和

(e) 有适当的机制在需要时向 相关监管机构提供风险评估。

6. 简化的尽职调查（“SDD”）

6.1 如果 Doo Prime 确定 ML 和 TF 风险较低，Doo Prime 可能会采用简化的尽职调查 (“SDD”) 方法。

6.2 可应用 SDD 的客户有：

(a) 金融机构；

(b) 一个机构：

(i) 在同等司法管辖区成立；

(ii) 经营类似于金融机构经营的业务；

(iii) 与任何监管机构类似职能，在该司法管辖区的机构监督监管监控是否遵守该要求；

(c) 在任何证券交易所上市的公司；

(d) 一种投资工具，其中负责对投资工具的所有投资者执行与 CDD 措施类似的措施的人是：

(i) 金融机构；

(ii) 成立或成立的机构，该机构：

- 已采取措施确保遵守与该适用的法规和条例规定的要求类似的要求； 和
- 受到监督以遵守这些要求。

(e) 政府或任何公共机构； 或

(f) 同等司法管辖区的政府或同等司法管辖区内执行与公共机构类似职能的机构。

6.3 在 SDD 的情况下，我们将：

(a) 识别客户并验证客户的身份；

(b) 如果要建立业务关系并且其目的和预期性质不明显，获取有关与我们的业务关系的目的和预期性质的信息； 和

(c) 如某人声称是代表该客户行事，

(i) 识别该人并采取合理措施核实该人的身份； 和

(ii) 核实该人代表客户行事的权力。

7. 加强尽职调查（“EDD”）

7.1 如果 Doo Prime 确定 ML 和 TF 风险很高，Doo Prime 应采用增强的尽职调查 (“EDD”) 方法和增强的持续监控。 在与高风险客户建立或继续业务关系和/或交易之前，需要得到 Doo Prime 高级管理层的批准。

7.2 EDD 适用的高风险情况包括：

(a) 客户风险因素：

(i) 业务关系是在不寻常的情况下进行的（例如，我们与客户之间存在无法解释的重大地理差异）；

(ii) 涉及没有明确合法商业目的的空壳工具的法人或法律安排；

(iii) 拥有名义股东或不记名股份的公司；

(iv) 现金密集型业务；

(v) 鉴于法人或法律安排的业务性质，该法人或法律安排的所有权结构显得异常或过于复杂； 或

(vi) 客户或客户的受益所有人是 PEP 或外国 PEP。

(b) 产品、服务、交易或交付渠道风险因素：

(i) 匿名交易（可能涉及现金）； 或

(ii) 从未知或不相关的第三方收到的频繁付款。

(c) 国家风险因素。 我们严禁与来自高风险国家的客户进行所有交易、银行转账和交易，包括但不限于：

(i) 由可靠来源，例如相互评估或详细评估报告，确定为没有有效的反洗钱和反恐融资系统的国家或司法管辖区；

(ii) 金融行动特别工作组确定的国家；

(iii) 被可靠来源确定为存在严重腐败或其他犯罪活动的国家或司法管辖区；

(iv) 受到例如联合国制裁、禁运或类似措施的国家或司法管辖区； 或

(v) 由可靠来源确定为恐怖活动提供资金或支持的国家、司法管辖区或地理区域，或指定恐怖组织开展活动的国家、司法管辖区或地理区域。

7.3 Doo Prime 保留从我们的独立来源获取信息以加强尽职调查措施的权利。 这包括但不限于：

(a) 获取有关客户的其他信息（例如职业、资产数量、所有权和控制结构、客户或受益所有人的声誉、可通过公共数据库、互联网等获得的信息），并更定期更新客户和受益所有人的身份数据；

(b) 获取有关业务关系和交易的预期性质、目的和背景的更多信息；

(c) 获取有关客户资金来源或财富来源的信息；

(d) 获取有关预期或已执行交易的原因的信息； 和/或

(e) 要求通过客户名下的账户在符合类似 CDD 标准的银行开立第一笔付款。

7.4 我们的 EDD 需要：

7.4.1 **增加为客户尽职调查而获取的信息数量**：

(a) 关于客户或实益拥有人的身份，或所有权和控制结构，以确信与该关系相关的风险是众所周知的。 这可能包括获取和评估有关客户或受益所有人声誉的信息，以及评估对客户或受益所有人的任何负面指控。 示例包括：有关家庭成员和密切商业伙伴的信息； 有关客户或实益拥有人过去和现在的业务活动的信息； 和不利的媒体搜索；

(b) 关于业务关系的预期性质，确定业务关系的性质和目的是否合法，并帮助公司获得更完整的客户风险概况。 它包括获取以下信息：

(i) 可能通过账户进行的交易的数量、规模和频率，以便能够发现可能引起怀疑的偏差，并在适当的情况下要求提供证据；

(ii) 客户寻找特定产品或服务的原因，特别是在不清楚为什么无法以其他方式或在不同司法管辖区更好地满足客户需求的情况下；

(iii) 资金去向；

(iv) 客户或实益拥有人的业务性质，以更好地了解业务关系的可能性质。

7.4.2 **提高为客户尽职调查而获得的信息的质量，以确认客户或受益所有人的身份，包括：**

(a) 要求通过以客户名义在银行开立的账户进行首次付款；

(b) 确定客户的财富来源和业务关系中使用的资金来源不是犯罪活动的收益，并且与我们对客户的了解和业务关系的性质一致。 可以通过参考所得税申报表、经审计的账目副本、工资单、公共行为或独立和可信的媒体报道等方式核实资金或财富的来源；

(c) 增加审查频率，以确保我们继续能够管理与个人业务关系相关的风险，并帮助识别需要进一步审查的任何交易，包括：

(i) 增加审查业务关系的频率，以确定客户的风险状况是否发生变化以及风险是否仍然可控；

(ii) 获得高级管理人员/指定高级管理人员的批准以开始或继续业务关系，以确保高级管理人员了解我们面临的风险，并可以就他们管理该风险的能力程度做出明智的决定；

(iii) 更定期地审查业务关系，以确保识别、评估客户风险状况的任何变化，并在必要时采取行动；

(iv) 进行更频繁或更深入的交易监控，以识别任何可能导致涉嫌洗钱或恐怖主义融资的异常或意外交易。 这可能包括确定资金的目的地或确定某些交易的原因；

(d) 在与已通过强化尽职调查流程的客户开展任何业务之前，该官员将需要提供批准或拒绝以继续进行客户设置流程。

7.5 我们将对我们认为具有高风险的任何情况、客户或交易采取 EDD 措施。

7.6 **资金来源和财富来源**

7.6.1 财富来源是指个人全部财富（即总资产）的来源。

7.6.2. 资金来源是指作为个人与我们之间业务关系主体的特定资金或其他资产的来源（例如，作为业务关系的一部分投资、存入或电汇的金额）。

7.7 **如何将资金来源和财富来源纳入我们的 EDD 流程**

7.7.1 财富来源通常表明客户预期拥有的财富规模，以及个人如何获得此类财富的情况。 尽管我们可能没有关于未存放或由其处理的资产的具体信息，但可能会从个人、商业数据库或其他开放来源收集一般信息。

7.7.2 资金来源信息不应仅仅局限于了解资金可能从哪里转移，还应包括产生资金的活动。获得的信息应该是实质性的，并确定获得资金的来源或原因。

7.8 Doo Prime 的政策是不接受任何第三方的任何资金，但如果出现此类特殊情况，我们将进行 EDD 以识别和验证其最终受益所有人，包括法人、合伙企业、信托和其他法律安排。

8. 验证

8.1 在与客户建立关系之前，我们将通过我们的客户服务和风险管理部门对客户的上述信息进行核实和筛选。我们的 CDD 范围包括但不限于我们的零售客户、业务合作伙伴、董事会成员、股东和最终实益拥有人。 我们执行以下 CDD 措施：

(a) 通过独立的筛选系统识别、验证和筛选客户的身份和信息；

(b) 如果有与客户有关的受益所有人，识别并采取合理措施核实受益所有人的身份，以便我们确信我们知道受益所有人是谁，包括在客户是法人或信托的情况下 ，使我们能够了解法人或信托的所有权和控制结构的措施；

(c) 获取与我们建立的业务关系（如果有）的目的和预期性质的信息，除非目的和预期性质是显而易见的； 和

(d) 如果某人声称代表客户行事：

(i) 使用可靠和独立来源提供的文件、数据或信息识别该人并采取合理措施核实该人的身份； 和

(ii) 核实该人代表客户行事的权力；

(e) 如果我们认为身份验证不充分或我们需要与客户执行的交易相关的其他详细信息，我们保留要求客户提供更多详细信息的权利（包括但不限于银行对账单、银行账户证明、电子钱包或 电子货币报表）并保留我们不建立业务伙伴关系或进行任何进一步交易的权利。 如果客户拒绝提供所需信息，或提供虚假/误导性信息，我们可能会冻结客户账户、限制交易或账户活动、终止业务伙伴关系和/或向监管机构报告。 在对客户身份和交易细节进行满意验证后，将取消对账户施加的所有限制。

8.2 在身份验证过程中，我们会要求提供身份证明文件的原件和彩色扫描件； 如果我们认为有必要，我们也可能会要求提供一份以上的身份证明文件进行交叉验证。

8.3 当使用电子验证或客户没有亲自到场进行身份识别时，我们将进行额外的验证检查以管理冒充欺诈的风险。 该检查可能采取以下形式：

(a) 要求通过以客户名义在受监管信贷机构开立的账户进行第一笔付款；

(b) 在开户之前，通过已验证的家庭或企业号码与客户电话联系；

(c) 在已验证的地址与客户进行通信；

(d) 要求文件副本由适当的人核证。

8.4 如果我们无法对某人执行规定的身份识别程序，我们：

(a) 不得为该人开立账户；

(b) 不得与该人建立业务关系； 和

(c) 如果与该人已经存在业务关系，我们将终止现有业务关系。

9. 报告

9.1 如果在 14 个工作日内（如果出现第 4.4(d) 和 (e) 条，则为 2 个工作日）没有向我们提供或我们没有获得令人满意的个人身份或验证证据，我们将向相关监管机构提交可疑活动报告 。 除非 相关监管机构指示，否则我们不会继续进行交易。

9.2 如果我们有合理理由怀疑客户不是其声称的人，我们将在情况发生之日起的三个工作日内采取以下一项或多项措施：

(i) 收集有关客户的必要客户身份信息； 或

(ii) 从可靠和独立的来源核实已获得的有关客户的某些客户信息； 确保合理地确信客户是他或她声称的那个人。

9.3 在确定和实施适当的基于风险的系统和控制措施时，我们将考虑客户业务的性质、规模和复杂性以及我们可能合理面临的 ML 和 TF 风险类型，包括但不限于以下因素：

(a) 客户类型，包括 PEP；

(b) 指定服务的种类;

(c) 我们所提供指定服务的方法，包括任何新产品的开发、业务实践以及使用新技术或正在开发的技术;

(d) 我们所处理的外国司法管辖区，包括金融行动特别工作组确定的高风险司法管辖区。

9.4 如果发生以下任何一种情况：

(a) 可疑交易；

(b) 可疑活动；

(c) 洗钱实体进行的交易；

(d) 涉及恐怖主义财产的交易；

(e) 没有合法目的的交易；

(f) 我们的监管机构或审计师有合理理由怀疑其拥有的交易或未遂交易或信息涉及犯罪所得或与资助恐怖主义有关；或

(g) 第 3.2 条所述的任何交易；

该交易应暂停，并且未经该官员授权不得进行。如有任何可疑交易或活动，我们的前线员工应立即向该官员报告，如有需要，该官员会在 2 个工作日内向相关监管机构提交可疑活动报告或可疑交易报告。

9.5 如果发现可疑的洗钱信号，应暂停交易，未经官员授权不得进行。在进行适当调查后，如果我们认为存在任何潜在的严重 ML 和 TF 风险，该官员将向相关监管机构报告此事。如果我们认为某人进行 2 次或更多交易以规避第 4.4(b) 条所述的金额阈值，我们将向相关监管机构 提交可疑交易报告。在提交报告之前，我们将考虑以下因素：

(a) 进行交易的方式和形式；

(b) 每笔交易所涉及的货币金额；

(c) 交易中涉及的货币总额；

(d) 交易发生的期间；

(e) 交易之间的时间间隔；

(f) 发起或进行交易的地点；

(g) 有关人士对进行交易的方式或形式作出的任何解释。

9.6 **可疑活动报告和可疑交易报告处理程序**

9.6.1 在进行适当的调查后，该官员将考虑酌情将此事报告给监管机构。 向主管和有关当局的所有记录，应由主管保存，期限不少于监管机构结案后的 7 年。 可疑活动报告或者可疑交易报告应当包括：

(a) 参与可疑活动或交易的个人或实体的资料和联系方式；

(b) 可疑活动或交易的详情；

(c) 观察到的可疑活动或交易指标；和

(d) 可疑活动报告或可疑交易报告所述的主体在被问及交易或活动时提供的任何解释。

9.6.2 向相关监管机构提交可疑活动报告或可疑交易报告为我们提供了针对报告中披露的行为的 ML 和 TF 罪行的法定辩护，前提是：

(a) 可疑活动报告或可疑交易报告是在我们进行披露的行为之前进行的，并且该行为或交易是在获得 相关监管机构同意的情况下进行的；或

(b) 可疑活动报告或可疑交易报告是在我们进行披露的行为或交易之后进行的，并且报告是我们主动且在合理的情况下尽快进行的。

9.7 所有发出的通知都将严格保密处理。但是，请注意，在某些情况下，我们可能需要透露个人身份，例如法律强制要求我们这样做，因此无法保证匿名。

9.8 我们知道，如果某人在知道或是怀疑一项披露已经提交给相关监管机构的情况下，向任何其他人披露任何可能妨碍在披露后可能进行的任何调查事项（通常称为“泄密”），是一项罪行。客户对可能的可疑活动报告或可疑交易报告或调查的认识可能会影响未来调查可疑 ML 和 TF 操作的努力。因此，如果我们怀疑与 ML 和 TF 相关的交易，我们将在执行 CDD 程序时考虑到泄密风险。我们将确保我们的员工在进行 CDD 时了解并意识这些问题。

9.9 我们不得向任何其他人披露任何信息：

(a) 我们或我们的监管机构或审计师或个人对交易或未遂交易、或某项活动或未遂活动产生怀疑；或

(b) 根据适用的法规和条例向 相关监管机构提交报告；或

(c) 根据该适用的法规和条例向 相关监管机构提供的信息；或

(d) 任何其他信息对于被披露信息的人，可以合理地从中推断出 (a)-(c) 段中的任何情况。

9.10 第 9.9 条不适用于对以下人员的披露：

(a) Doo Prime 的高级职员、雇员或代理人，出于与我们履行职责相关的任何目的，已经或被要求根据适用的法规和条例进行报告或提供信息；或

(b) 为就披露获取法律意见或代理的目的而聘请的律师；或

(c) Doo Prime 的主管；或者

(d) 根据适用的法规和条例协助 相关监管机构的执法机构或任何其他人。

9.11 我们的官员的职责包括但不限于以下内容：

(a) 审查可疑交易的所有内部报告和异常报告，并根据所有可用信息，确定是否有必要向相关监管机构提交可疑活动报告或可疑交易报告；

(b) 保存与此类内部审查有关的所有记录；

(c) 指导员工在提交任何可疑活动报告或可疑交易报告时如何避免“泄密”；

(d) 作为与 相关监管机构、执法机构和任何其他与 ML 和 TF 预防和检测、调查或合规有关的主管当局的主要联系。

10. 持续的客户尽职调查和交易监控

10.1 我们将通过持续的客户尽职调查和交易监控进行持续监控，以确保遵守 AML 和 CTF 系统。我们将在任何触发事件时审查现有的客户尽职调查记录，并根据所采用的基于风险的方法维持适当的系统来监控交易。监控范围应与客户的 ML 和 TF 风险状况成比例。

10.2 持续 CDD

10.2.1 我们通过以下方式持续监控客户的活动：

(a) 不时审查为遵守客户尽职调查要求而获得的与客户有关的文件、数据和信息，以确保它们是最新的和相关的；

(b) 对为客户进行的交易进行适当的审查，以确保它们与我们对客户和客户业务、风险状况和资金来源的了解一致；和

(c) 识别复杂、金额异常大或模式异常或没有明显经济或合法目的且可能表明存在 ML 和 TF 的交易。

10.2.2 拥有

(a) 高 ML 和 TF 风险的客户应每 6 个月进行一次审查；

(b) 高 ML 和 TF 风险的客户应每 6 个月进行一次审查；

(c) 低 ML 和 TF 风险的客户应每 2 年进行一次审查；

或在我们认为必要的情况下进行更频繁的审查，以确保保留的客户尽职调查信息与我们对客户、客户业务、资金来源和风险状况的了解一致。

10.2.3 对所有被列为高风险的客户进行全面审查。这将需要建立以下内容：

- 重新确认地址
- 重新确认公司结构（如适用）
- 重新确认资金和财富来源
- 查看负面新闻
- 全面审查交易资料，包括要求的新产品

10.3 交易监控

10.3.1 我们保持合适的系统来监控和审查所有基于风险的方法进行的交易，我们将根据以下因素检查和审查交易是否正常：

(a) 其业务的规模和复杂性；

(b) 其业务产生的 ML 和 TF 风险；

(c) 其系统和控制的性质；

(d) 已经存在以满足其他业务需求的监控程序；和

(e) 所提供产品和服务的性质（包括交付或通信方式）。

10.3.2 我们定期审查其交易监控系统和流程的适用性和有效性，包括采用的参数和阈值。采用的参数和阈值包括以下因素：

(a) 交易的性质和类型（例如异常规模或频率）；

(b) 一系列交易的性质（例如，将单笔交易分成几笔现金存款）；

(c) 交易的对手方；

(d) 付款或收款的地理来源/目的地；

(e) 客户的正常账户活动或营业额；

(f) 客户的行为 - 交易活动的价值、数量或性质的突然和/或重大变化，例如受益人或目的地的变化；

(g) 客户的关联关系 - 在明显没有关联的账户或客户中识别共同的受益人和汇款人。

11. 记录保存

11.1 向官员提交的所有身份验证文件、交易记录、CDD 信息、ML 和 TF 报告的原件和复印件的记录，与可疑活动报告、可疑交易报告有关的所有文件，处理可疑交易报告和其结果和其他文件手下的人员 在与客户的业务关系结束后至少 7 年内被整理并保密。

11.2 每个客户的记录保存要求如下：

(a) 我们必须保留以下文件的原件或副本：

(i) 文件，以及在识别和验证客户身份过程中获得的数据和信息的记录；客户的实益拥有人；声称代表客户行事的人；和

(ii) 与客户的业务关系和与客户及客户的任何实益拥有人的业务往来有关的文件；和

(b) 上述 (a) 分段中提及的文件和记录必须在与客户的业务关系持续期间保存，并从业务关系结束之日起至少保存七年。

11.3 每笔交易的记录保存要求如下：

(a) 我们将保留文件的原件或副本，以及与交易相关的数据和信息的记录，包括但不限于以下内容：

(i) 交易的性质；

(ii) 交易金额及其计价货币；

(iii) 进行交易的日期；

(iv) 关于以下每人的姓名、地址和职业、业务或主要活动（视情况而定）：

(aa) 进行交易；和

(ab) 如果我们有合理理由相信该人正在代表任何其他人进行交易，则交易是为谁或代表为了谁的最终利益而进行的；

(v) 交易中涉及与我们的任何账户/服务的类型和识别号；

(vi) 如果交易涉及货币以外的流通票据：

(aa) 票据的出票人；

(bb) 开票的机构名称；

(cc) 收款人名称（如有）；

(dd) 票据的金额和日期；和

(ee) 票据的编号（若有）和票据上出现的任何代言的细节；

(vii) Doo Prime 的姓名和地址，以及准备相关记录或部分记录的 Doo Prime 的每个高级职员、雇员或代理人的姓名和地址；

(viii) 与该交易有关的任何其他信息。

(b) 根据 (a) 项要求保存的记录必须自交易完成之日起至少保存七年，无论业务关系是否在此期间结束。

12. AML 和 CTF 审查过程

12.1 将根据 Refinitiv Limited 的 World-Check One 筛选系统提供的制裁名单、政治公众人物、监管执法、执法、洗钱、恐怖主义融资、不良媒体报道对客户进行筛选。 客户将被添加到 World-Check One 的持续监控列表中，系统将每 12 小时自动搜索他们的详细信息。 每当有任何正匹配时，我们都会收到警报。

12.2 我们审查：

(a) 在建立关系时，我们会查看客户和客户的任何受益所有人对照当前数据库；

(b) 客户和客户的任何实益拥有人在切实可行的情况下尽快对数据库的所有新指定和任何更新指定；和

(c) 跨境电汇中的所有相关方在执行转账前对照当前数据库.

12.3 如有任何涉恐怖主义融资、扩散融资和违反制裁的行为嫌疑，我们将向相关监管机构提交可疑活动或可疑交易报告。我们将通过向相关监管机构提交可疑活动报告或可疑交易报告的方式报告任何资产被冻结或根据金融制裁要求采取的行动。

13. AML 和 CTF 审计职能

13.1 官员和我们的合规部门每年对我们的 AML 和 CTF 政策进行内部审计，以确保我们的 AML 和 CTF 政策得到更新。我们了解我们遵守该适用的法规和条例的法定责任，我们将至少每年更新和审查我们的 AML 和 CTF 政策一次。

13.2 我们将定期识别和评估可能出现的与以下相关的 ML 和 TF 风险：

(a) 我们合理预期在其业务过程中可能面临的洗钱和恐怖主义融资风险的性质和程度；

(b) 我们业务的性质、规模和复杂度；

(c) 开发新产品和新业务做法，包括新的交付机制；和

(d) 对新产品和现有产品使用新技术或正在开发的技术。

14. 培训计划

14.1 Doo Prime 的所有相关人员都将接受本 AML 和 CTF 政策中提供的相关政策和知识培训。此外，Doo Prime 的所有相关员工都将了解他们的工作描述，并将接受有关他们在洗钱和资助恐怖主义交易方面的职责的培训。他们将被指导如何识别和处理可能涉及洗钱和资助恐怖主义的交易。

14.2 培训范围

14.2.1 员工将被告知：

(a) 我们的法定义务及其法定义务以及未能根据适用的法规和条例和条例报告可疑交易的可能后果；

(b) 根据该适用的法规和条例和条例与我们有关的任何其他法定和监管义务，以及违反这些义务的可能后果；

(c) 我们与 AML 和 CTF 有关的政策和程序，包括可疑活动和交易识别和报告;

(d) ML 和 TF 中的任何新出现的技术，方法和趋势，只要工作人员需要这些信息来履行其在 AML 和 CTF 方面的各自职责;

(e) 升级程序，即一旦识别出 ML 和 TF 风险应该做什么;

(f) 员工在我们的合规工作中扮演什么角色以及如何执行这些工作;

(g) 记录保存和记录保留政策；和

(h) 不遵守该适用的法规和条例的纪律处分（民事和刑事）。

14.2.2 对合适的员工或员工群体进行重点培训将使 Doo Prime 和高级管理层能够有效地实施其 AML 和 CTF 系统。以下培训领域可能适合某些员工群体:

(a) 所有新工作人员（不论资历）

(i) ML 和 TF 的背景介绍以及 AML 和 CTF 对我们的重要性；和

(ii) 识别并向官员报告可疑交易的需要和义务，以及“举报”罪。

(b) 前线员工（即直接与客户来往的员工）

(i) 他们在地产代理公司的 AML 和 CTF 战略中扮演的角色的重要性是与潜在的洗钱者和参与 TF 的人接触的第一点;

(ii) 地产代理公司有关客户尽职调查的政策和程序以及与其工作职责相关的记录保存要求;

(iii) 识别不同情况下可能引起怀疑的异常活动的指南或提示；和

(iv) 报告异常活动的相关政策和程序，包括可能需要格外警惕的报告线路和情况。

(c) 后勤人员

(i) 关于客户验证和相关处理程序的适当培训；和

(ii) 识别异常活动的方法，包括异常结算、付款或交付指令。

(d) 管理人员（包括内部审计人员）

(i) 涵盖 AML 和 CTF 制度各个方面的更高级别的培训；

(ii) 适用于我们的 AML 和 CTF 要求的具体培训；和

(iii) 就其监督或管理员工、审计系统和进行随机检查以及向相关监管机构报告可疑交易的职责进行专门培训。

(e) 官员

(i) 有关员工评估提交给他们的可疑交易报告和向相关监管机构报告可疑交易的职责的具体培训；

(ii) 培训以跟上 AML 和 CTF 的要求/发展；

(iii) 接收公司人员关于可疑活动的报告；和

(iv) 与适当的工作人员协调所需的反洗钱审查/会议。

14.3 我们将监控培训的有效性。这可以通过以下方式实现：

(a) 测试员工对我们打击 ML 和 TF 的政策和程序的理解，对他们的法定和监管义务的理解，以及他们识别可疑交易的能力；

(b) 监控员工对我们的 AML 和 CTF 系统的遵守情况以及内部报告的质量和数量，以便确定进一步的培训需求并采取适当的行动；和

(c) 监督出勤率并跟进无正当理由错过此类培训的员工。

14.4 我们每年至少对所有相关员工进行一次反洗钱培训、研讨会和评估。

14.5 我们应观察并记录我们接受过充分培训的员工的培训时间或最后一次培训时间，然后为他们提供额外的、必要的和充分的培训。

15. 语言和修改

15.1 本 AML 和 CTF 政策的官方语言为英语。 Doo Prime 可能会以其他语言提供本 AML 和 CTF 政策，仅供参考，如果本 AML 和 CTF 政策的英文版本与任何其他语言版本之间存在任何不一致或差异，以英文版本为准。

15.2 客户承认 Doo Prime 保留随时修改或更新本 AML 和 CTF 政策的权利，恕不另行通知客户。AML 和 CTF 政策的修订应立即生效，并在 Doo Prime 网站上发布 AML 和 CTF 政策后对客户具有法律约束力。客户承诺在 Doo Prime 网站上定期查看本 AML 和 CTF 政策。

(本页的其余部分故意留空)