Email: support@lordprime.io
Website: lordprime.io

AML & KYC POLICY

1. INTRODUCTION

1.1. The term "money laundering" encompasses all procedures aimed at concealing the origin of criminal proceeds to create the impression that they were obtained from a legitimate source. Lord Prime LTD. (the "Company") is committed to identifying, managing, and mitigating risks associated with money laundering and terrorist financing. The Company has implemented a strict policy aimed at identifying, preventing, or mitigating risks related to any suspicious activities carried out by clients.

1.2. The Company is obligated to continuously monitor its exposure to the risk of money laundering and terrorist financing.

1.3. The Company believes that knowing its customer well and thoroughly understanding their instructions provides better opportunities to assess risks and identify suspicious actions.

2. ANTI-MONEY LAUNDERING POLICY

2.1. In accordance with all regulatory requirements such as identification and knowing our customers:

2.2. The Company does not permit the opening of anonymous or numbered accounts;

2.3. The Company does not open accounts for individuals with a criminal record, those under investigation, or serving a prison sentence;

2.4. The Company is obligated to identify, monitor, and report all suspicious transactions;

2.5. The Company is required to keep all transaction records for at least 3 years after the termination of contractual relationships with clients;

2.6. The Company must continually train its employees to recognize any suspicious transactions and report them to the authorities in accordance with applicable laws and regulations;

2.7. The Company has the right to request and verify identification documents from its clients before opening an account and processing payments;

2.8. The Company is obligated to deny the Client access to the trading platform and fund transfers at any time if the Client is suspected of and/or identified as being involved in criminal activity or money laundering in any way.

2.9. All Clients are required to comply with the Company's anti-money laundering policy. By confirming the registration of an account, the Client unconditionally agrees to comply with all requirements of the Company's anti-money laundering policy.

2.10. As a responsible member of the financial community, the Company makes every effort to protect its clients and maintain an impeccable reputation when it comes to anti-money laundering measures and international financial sanctions.

Email: support@lordprime.io
Website: lordprime.io

3. RISK ASSESSMENT

3.1. The overall goal is to understand from the outset who our partners are, where they operate, what they do, and the expected level of their interaction with us. There are additional risk considerations related to the position of relevant jurisdictions, their regulation, and status regarding their inherent risks of money laundering (ML) and terrorist financing (TF), as well as the effectiveness of their anti-money laundering and counter-terrorist financing (AML/CTF) enforcement regime.

3.2. Money laundering (ML) is the process of concealing or attempting to conceal the true origin of proceeds from criminal activities and their ownership to legitimize such funds.

3.3. The Anti-Money Laundering (AML) policy is implemented in three stages:

3.3.1. Placement – the physical disposal of cash proceeds derived from criminal activity. Among other things, placement may involve converting the proceeds into financial instruments or bank deposits in such a way that it does not arouse suspicion.

3.3.2. Layering – the separation of illicit proceeds from their source by creating complex layers of financial transactions designed to obscure the audit trail and provide anonymity;

3.3.3. Integration – the process of ensuring the apparent legitimacy of illicitly obtained income. If the layering process is successful, integration schemes return the laundered proceeds back into the economy in such a way that they re-enter the financial system as legitimate business funds.

3.4. Terrorist Financing (TF). Terrorist financing means providing or collecting funds by any means, directly or indirectly, with the intention that they be used or knowing that they will be used, in whole or in part, to carry out any offenses related to terrorism.

3.5. There are factors indicating a higher risk of ML/TF activities, such as geographical location, partners, and the type of services provided. When assessing ML/TF risks, the aforementioned factors are prioritized to identify risk variables. When weighing factors, we must ensure that no single factor disproportionately influences the assessment, economic considerations or profit motives do not affect risk assessment, and situations identified by national law or risk assessments as always posing a high ML risk cannot be overridden by us.

3.6. Meanwhile, there are some circumstances where the risk of money laundering or terrorist financing may be lower. In such circumstances, given an adequate risk analysis, we may apply simplified anti- money laundering measures: for example, a low ML/TF risk registration country, or partners with whom we have long-term and active business relationships. However, the assessment of a jurisdiction as low risk only allows for some reduction in the level of due diligence – it is not a complete exemption from applying CDD measures regarding partner identification.

3.7. The most important procedures that the Company implements to achieve these goals are as follows:

3.7.1. Client identification and due diligence procedures;

3.7.2. Record-keeping procedures concerning the identity of clients and their transactions;
3.7.3. Internal reporting procedures to a competent person (MLRO) appointed to receive and consider information that gives grounds to suspect a client of money laundering;
3.7.4. Adequate internal control and risk management procedures aimed at preventing activities related to money laundering;
3.7.5. Detailed scrutiny of each transaction that, by its nature, is considered vulnerable to money laundering, especially complex or unusually large transactions, as well as transactions that are conducted without any apparent economic or lawful purpose;
3.7.6. Measures to inform employees about the above-mentioned procedures for preventing money laundering and legislation related to money laundering; and conducting regular training of employees to help them recognize and handle transactions suspected of being related to money laundering.
3.8. We will conduct our KYC/CDD and activity monitoring based on a risk-based approach:
3.8.1. For some clients who, in our opinion, pose a low ML/TF risk, simplified KYC/CDD and monitoring procedures may be applied;
3.8.2. In the case of high-risk profiles, enhanced KYC/CDD measures (including but not limited to additional verification information or confirmation of funding sources) and enhanced monitoring will be applied.
3.8.3. In cases where ML/TF risks are higher, we must apply enhanced due diligence measures appropriate to the identified risks.
3.9. In particular, we must increase the degree and nature of determining business relationships. Examples of EDD measures to be applied to high-risk business relationships include:
3.9.1. Obtaining and, where necessary, verifying additional information about the potential Client and more frequent updating of identification data of the potential client and any beneficial owner;
3.9.2. Obtaining additional information about the intended nature of the business relationship;
3.9.3. Obtaining information on the source of the Client's funds;
3.9.4. Obtaining information on the reasons for planned or completed transactions;
3.9.5. Obtaining senior management approval to start or continue the business relationship.
3.10. Clients who are considered to be high risk include, but are not limited to:
3.11. Clients whose identification process is incomplete;

3.12. Clients with discrepancies in the provided identification information and documents;
3.13. Clients classified as PEPS (politically exposed persons) or known close associates of PEPS;
3.14. Clients who have been prosecuted for financial crimes;
3.15. Clients who are citizens or residents of territories under enhanced FATF monitoring;
3.16. Clients listed as terrorists or in other sanctions lists: the consolidated sanctions list of the United Nations Security Council, the consolidated list of individuals, groups, and entities of the EU, the sanctions lists of the U.S. Department of Treasury, Office of Foreign Assets Control (OFAC), the U.S. Treasury Department, the Financial Crimes Enforcement Network (FinCEN), the UK Treasury (HMT), the Office of Financial Sanctions Implementation, the “consolidated list of targets”).
3.17. When dealing with the potential ML risks of those Clients identified as higher risk through our risk assessment process, we may apply one or more of the following measures and controls:
3.18. Increasing our awareness of high-risk situations within the Company’s business lines;
3.19. Enhanced levels of KYC or CDD;
3.20. Higher level of approval for establishing business relationships;
3.21. Enhanced transaction monitoring;
3.22. Increased levels of ongoing control and scrutiny of the relationship.
3.23. Applying one of the established risk criteria does not necessarily mean we will implement specific control measures targeting each risk criterion outlined in this KYC/AML Policy.
3.24. Receiving funds payable through shell accounts or any financial institutions from restricted jurisdictions is prohibited. We will report all transactions involving suspicious banks and territories. Clients are prohibited from using our services to pay for assets obtained from any illegal or otherwise restricted services and products under applicable law.
3.25. Restricted jurisdictions. We do not provide services to any person who is a citizen or resident (tax or otherwise) of any jurisdiction that is:
3.26. A restricted jurisdiction;
3.27. Any country or territory subject to comprehensive country or territory-wide sanctions. Risk criteria.
3.28. Lord Prime denies entering into an Agreement and providing services to any individual or legal entity if the KYC and CDD procedures identify the prospective or existing client as a citizen or resident of the jurisdictions listed herein.
3.29. Clients must assume that all information provided to the Company is available to competent regulatory authorities in:
the country of the Company’s registration;

the country of origin of any funds transferred to the Company;
the country of destination of any funds returned by the Company or withdrawn from it.
Payments from third parties or anonymous payments are not accepted. If the Company is not confident that the Client is the sender of the funds, it reserves the right to reject the transfer and return it to the sender, deducting any transfer fees or other charges. The Company also reserves the right to immediately close your account provided to us.

4. CUSTOMER IDENTIFICATION AND VERIFICATION (KYC AND CDD)

4.1. The purpose of KYC and CDD is to identify customers and verify their identities. Lord Prime may ask you to provide identification information and specific documents either during registration as a Client or periodically for the purpose of record keeping and ongoing CDD and procedures.

4.2. The following documents may be required from natural persons:

4.2.1. National passport or its notarized copy;

4.2.2. Proof of residence (residence certificate, utility bill, or bank statement indicating the place of residence) or its notarized translation issued within 3 months prior to the date of submission to us;

4.2.3. Expired lease agreement;

4.2.4. Valid foreign resident ID or valid driver's license.

4.3. Legal entities may be required to provide the following documents:

4.3.1. Notarized extract from the trade register (or equivalent) in English;

4.3.2. Charter in English;

4.3.3. Stock certificates;

4.3.4. Appointment decision of the director;

4.3.5. National passport of the Client's director or its notarized copy with an apostille;

4.3.6. National passport of the beneficial owner of the Client;

4.4. If the director or owner of the Client is a legal entity, and the Client is also a legal entity, all the above-mentioned documents must be provided.

4.4.1. Directors of companies, as well as other persons with significant control, undergo enhanced due diligence procedures, including screening for PEP compliance and sanctions lists. When another person conducts asset transactions by proxy, this person, as well as the company director, must also undergo screening for PEP compliance and sanctions lists.

4.4.2. Beneficiary (ultimate beneficial owner). AML rules define beneficial owners as natural persons who own or control more than 25% of the shares of legal entities or partnerships or otherwise own or control a partner.

4.4.3. These individuals must be identified, and reasonable measures must be taken to verify their identities. It is necessary to know the names of all individual beneficial owners who own or control more than 25% of the company's shares or voting rights (even if these shares are owned indirectly) or who otherwise control the company's

management.
4.4.4. Our company's obligation to verify the identity of the beneficial owner consists of taking reasonable measures to ensure that we know who the beneficial owner is. We ourselves decide whether it is appropriate, given the risk of money laundering or terrorism financing associated with business relationships, to use publicly available records of beneficial owners, request relevant data from our employees, or require confirmation of the beneficial owner's identity. based on documentary information obtained from a reliable source independent of partners or obtain information in any other way.
4.5. In low-risk situations, it may be reasonable to verify the identity of the beneficial owner based on information provided by partners. This may include information provided by partners (including trusted persons or other representatives whose identities have been confirmed) about their identity and confirmation that they are known to partners. All documents provided by the Client to the Company must be: issued by government authorities; have a photo of the owner, full name, document number, or personal number of the owner and date of birth (in its absence, we request additional documentation, if available, with the date of birth); be valid and current.
4.6. If identity is confirmed electronically, we may apply additional verification to reduce the risk of fraud by impersonation. For instance, one such verification may require certified copies of documents by the relevant authority.
4.7. Third-party authentication. As part of the verification process, we reserve the right to engage one or more appropriate third-party service providers to assist us in verifying the authenticity and/or verifying the validity of documents and other additional information provided by you.
4.8. Lord Prime reserves the right to conduct identity verification by cross-referencing certain identification data with documents or information obtained from a reliable source independent of the Client.
4.9. Authentication through visitation. We reserve the right to visit the premises where you, the controlling person, or the beneficial owner of assets conduct your business activities.
4.10. Enhanced compliance with KYC/CDD requirements. In addition to standard KYC/CDD procedures, we also reserve the right to apply additional KYC/CDD measures, as described in this KYC/AML Policy, when suspicions arise regarding AML/CFT, irrespective of any deviations, exemptions, or thresholds. Doubts arise about the accuracy or adequacy of previously obtained identification data and documents; You provide new identification data or documents.
4.11. Information Updates. To implement this KYC/AML Policy and mitigate AML/CFT risks, as well as to ensure that the information we hold about you is always accurate and up to date, you must provide us with updated identification information and relevant documents to continue using our services in any of the following circumstances:

Any time you receive a new identity document to replace the previous one;
Any time you change your personal identification number (if applicable);
Any time you change your name or part of it;
Any time you change your phone number, email address, or residential address; Any time a new director and/or beneficial owner (if the Client is a legal entity) is appointed.

4.12. Anti-Money Laundering Policy. When using our services, you will also be prompted to update your identification data:
Once every 12 months if you are a low or medium-risk client;
Once every 6 months if you are a high-risk client.

4.13. We take all reasonable measures to protect your identification information and provide documents in accordance with applicable laws and regulations.

5. AMENDMENTS TO THIS POLICY

5.1. We reserve the right to make changes to this KYC/AML Policy at any time with immediate effect by adopting an updated version of the Policy. All such changes will come into effect after they have been approved by an authorized representative of the Company and updated on the Company's website. If you continue to use the Services, you are deemed to accept any such changes. Where possible, the Company may send you a notification of changes to the KYC/AML policy by email to your last known email address, and such notification takes effect immediately.

5.2. It is important for you to regularly review this KYC/AML Policy to ensure that you are familiar with the current terms and/or any changes made to them. If you disagree with any changes, you must cease using our Services and contact us to terminate the Agreement.

6. CONTACT US

If you require further information and/or have any questions about KYC, please direct your inquiry and/or questions to support@lordprime.io.