LANESRA LTD t/a UBUNTU MARKETS

(**the "Provider**")

ANTI MONEY LAUNDERING POLICY

Last Update: 2024-03-14

TABLE OF CONTENTS

1 APPLICATION OF THE POLICY

1.1 This policy applies to all Lanesra Ltd officers (the Company), employees, appointed producers and products and services offered by Ubuntu We Sizwe 247 (Pty) Ltd.

2 PURPOSE OF THE POLICY

2.1 The purpose of this Anti- Money Laundering (AML) compliance policy ("Policy") is to formally document the Company's commitment to the Financial Intelligence Centre Act 38 of 2001 (FICA) as amended by the Financial Intelligence Centre Amendment Act, 2017 (the FICA Amendment) and its associated regulations and guidance notes as well as the Prevention of Organised Crime Act No 24 of 1999 (POCA) and the Protection of Constitutional Democracy Against Terrorist Related Activities Act 33 of 2004(POCDATARA).

2.2 All business units and locations within the Company will cooperate to create a cohesive effort in the fight against money laundering. Each business unit and location has implemented risk-based procedures reasonably expected to prevent, detect and cause the reporting of transactions required under the FICA. All efforts exerted will be documented and retained in accordance with the FICA. The AML Compliance Committee is responsible for initiating Suspicious Activity Reports ("SARs") or other required reporting to the appropriate law enforcement or regulatory agencies. Any contacts by law enforcement or regulatory agencies related to the Policy shall be directed to the AML Compliance Committee. It is the policy of the Company to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company is committed to AML compliance in accordance with applicable law and requires its officers, employees and appointed producers to adhere to these standards in preventing the use of its products and services for money laundering purposes.

3 DEFINITIONS

3.1 **Money laundering** is any process designed to conceal or disguise the true origins of criminally derived proceeds so that the unlawful proceeds appear to have been derived from legitimate origins or constitute legitimate assets.

3.2 Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

4 RISK MANAGEMENT AND COMPLIANCE PROGRAMME (RMCP)

4.1 The RMCP encompasses the processes and procedures employed by the Company to identify, assess, monitor, mitigate and manage any risks related to money laundering and the financing of terrorist activities.

5 AML COMPLIANCE COMMITTEE

5.1 The AML Compliance Committee, with full responsibility for the Policy shall be comprised of the Company shareholders, Corporate Attorney and the Head of Compliance. The Head of Compliance shall also hold the title Chief AML Officer, and shall have authority to sign as such. The duties of the AML Compliance Committee with respect to the Policy shall include, but are not limited to, the design and implementation of as well as updating the Policy as required; dissemination of information to officers, employees and appointed producers of the Company, training of officers, employees and appointed producers; monitoring the compliance of the Company operating units and appointed producers, maintaining necessary and appropriate records, filing of SARs when warranted; and independent testing of the operation of the Policy. Each Company business unit shall appoint a contact person to interact directly with the AML Compliance Committee to assist the Committee with investigations, monitoring and as otherwise requested.

5.2 MONITORING AND REPORTING

Transaction based monitoring will occur within the appropriate business units of the Company. All reports will be documented and retained in accordance with the FICA requirements.

6 SUSPICIOUS ACTIVITY

6.1 There are signs of suspicious activity that suggest money laundering. These are commonly referred to as **"red flags."** If a red flag is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the AML Compliance Committee. Examples of red flags are:

6.1.1 The customer exhibits unusual concern regarding the firm's compliance with government reporting requirements and the firm's AML policies, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning business activities or furnishes unusual or suspect identification or business documents.

6.1.2 The customer wishes to engage in transactions that lack business sense or apparent investment strategy or are inconsistent with the customer's stated business strategy.

6.1.3 The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.

6.1.4 Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.

6.1.5 The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.

6.1.6 The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

6.1.7 The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.

6.1.8 The customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

6.1.9 The customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents, or asks for exemptions from the firm's policies relating to the deposit of cash and cash equivalents.

6.1.10 The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.

6.1.11 For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

6.1.12 The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force.

6.1.13 The customer's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity

6.1.14 The customer's account shows numerous currency or cashier's check transactions aggregating to significant sums.

6.1.15 The customer's account has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.

6.1.16 The customer's account has wire transfers that have no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.

6.1.17 The customer's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose.

6.1.18 The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

6.1.19 The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

6.1.20 The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.

6.1.21 The customer requests that a transaction be processed in such a manner to avoid the firm's normal documentation requirements.

6.1.22 The customer, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence to ensure the legitimacy of the customer's activity.)

6.1.23 The customer's account shows an unexplained high level of account activity with very low levels of securities transactions.

6.1.24 Attempt to borrow maximum cash value of a single premium policy soon after purchase.

6.1.25 If the appointed producer:

6.1.25.1 exhibits a dramatic or unexpected increase in sales (particularly of single premium contacts);

6.1.25.2 has consistently high activity in single premium contracts in excess of company averages;

6.1.25.3 exhibits a sudden change in lifestyle;

6.1.25.4 requests client documentation to be delivered to the agent.

7 INVESTIGATION

7.1 Upon notification to the AML Compliance Committee of a match to the OFAC SDN List or possible suspicious activity, an investigation will be commenced to determine if a report should be made to appropriate law enforcement or regulatory agencies. The investigation will include, but not necessarily be limited to, review of all available information, such as payment history, birth dates, and address. If the results of the investigation warrant, a recommendation will be made to the AML Compliance Committee to file a blocked asset and/or a SAR with the appropriate law enforcement or regulatory agency. The AML Compliance Committee is responsible for any notice or filing with law enforcement or regulatory agency. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or SAR filing with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

8 CUSTOMER IDENTIFICATION PROGRAM

8.1 Client identification and verification is a crucial part of any effective money laundering control system.

8.2 The Company has adopted a Customer Identification Program (CIP). The Company will provide notice that they will seek identification information; collect certain minimum customer identification information from each customer, record such information and the verification methods and results; and compare customer identification information with OFAC.

8.3 Notice to Customers

8.3.1 The Company will provide notice to customers that it is requesting information from them to verify their identities, as required by applicable law.

8.4 Verifying Information

8.4.1 Verification is the process where one is required to collect documents to serve as proof of information of the client. These documents will serve as corroboration to any documents in the clients' possession.

8.4.2 In instances where we don't meet the client in person (due to internet or telephone correspondence), we will take reasonable steps to establish an existence or to verify the identity of the client taking into account the relevant guidance notes.

8.4.3 In circumstances where it is necessary to obtain additional information from a client to identify the proceeds of unlawful activities or money laundering activities, in addition to the source of funds that must be obtained, the following information and documentation may be obtained from natural person, legal persons, partnerships or trusts:

8.4.3.1 Natural Persons:

8.4.3.1.1 The nature and extent of the business activity that such a person may be involved in; and

8.4.3.1.2 The nature and extent of possible transactions that such a person may be involved in with the accountable institution.

8.4.3.2 Natural Persons (Foreign Nationals):

8.4.3.2.1 The nature and extent of the business activity that such a person may be involved in;

8.4.3.2.2 The nature and extent of possible transaction that such a person may be involved in with the accountable institution;

8.4.3.2.3 The purpose of such a person being in the Republic;

8.4.3.2.4 The time duration for such a person stay in the Republic;

8.4.3.2.5 A copy of the passport of such a person reflecting his/her entrance into the Republic and applicable visa (if relevant); and

8.4.3.2.6 If applicable, a copy of the work permit in the Republic, of such a person.

8.4.3.3 Legal Person, Other Legal Entities, Partnerships Or Trusts:

8.4.3.3.1 The nature and extent of the business activity that the entity may be involved in;

8.4.3.3.2 The nature and extent of possible transactions that the entity may be involved in with the accountable institution;

8.4.3.3.3 If the entity operated out of various branches and in various jurisdictions, the details in this regard must be obtained and noted

8.4.3.4 Legal Persons (Foreign):

8.4.3.4.1 The nature and extent of the business activity that the entity may be involved in;

8.4.3.4.2 The nature and extent of possible transactions that the entity may be involved in with the accountable institution;

8.4.3.4.3 If the entity operates out of various branches and in various jurisdictions, the detail in this regard must be obtained and noted.

8.5 CUSTOMERS WHO REFUSE TO PROVIDE INFORMATION

8.5.1 If a customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the appointed agent shall notify their New Business team. The Company New Business team will decline the application and notify the AML Compliance Committee.

9 CHECKING THE OFFICE OF FOREIGN ASSETS CONTROL ("OFAC") LIST

9.1 For all:

9.1.1 new applications received and on an ongoing basis;

9.1.2 disbursements;

9.1.3 new producers appointed; or

9.1.4 new employees; the Company will check to ensure that a person or entity does not appear on Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List (SDN List) and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC Web Site.

9.1.5 The Company may contract with World-Check to ensure speed and accuracy in the checks. The Company will also review existing policyholders, producers and employees against these lists on a periodic basis. The frequency of the reviews will be documented and retained. In the event of a match to the SDN List or other OFAC List, the business unit will conduct a review of the circumstances where such match has been identified. If the business unit is unable to confirm that the match is a false positive, the AML Committee shall be notified.

10 RECORDKEEPING

10.1 The AML Compliance Committee will be responsible to ensure that records of all dealings with clients including the identity of the client or the persons acting on behalf of the clients are maintained. Records of the details of transactions and parties to the transactions will be maintained properly, and SARs and Blocked Property Reports will be filed as required. The Company will maintain AML records on file for at least five years.

11 TRAINING

11.1 The Company shall provide anti-money laundering training to its officers, employees and appointed producers to ensure awareness of requirements under the FICA.

11.2 The training will include, at a minimum:

11.2.1 how to identify red flags and signs of money laundering;

11.2.2 what roles the officers, employees and appointed producers have

11.2.3 the Company compliance efforts;

11.2.4 how to perform such duties and responsibilities;

11.2.5 what to do once a red flag or suspicious activity is detected;

11.2.6 the Company record retention policy;

11.2.7 and the disciplinary consequences for non-compliance with the Act and this Policy.

11.3 In addition, each affected area will provide enhanced training in accordance with the procedures developed in each area for officers and employees reasonably expected to handle money, requests, or processing that may bring them into contact with information designated above.

11.4 Training will be conducted on an annual basis.

11.5 The AML Compliance Committee will determine the ongoing training requirements and ensure written procedures are updated to reflect any changes required in such training. The Company will maintain records to document that training has occurred.

12 TESTING OF THE POLICY

12.1 The testing of the Policy may be conducted by an outside independent third party annually. Any findings will be reported to the AML Compliance Committee and Senior Management for appropriate action.

13 ADMINISTRATION

13.1 The AML Compliance Committee is responsible for the administration, revision, interpretation, and application of this Policy. The Policy may be updated from time in line with changes in legislation or to better improve the anti-money laundering processes of the Company .Once updated the policy will be available to staff.

14 DISCIPLINARY PROCEEDINGS

14.1 Any employee of the Company found to be in contravention of the requirements and provisions outlined in this policy shall be subject to internal disciplinary proceedings as well as administrative sanctions / penalties as may be required by the Act.