AML POLICY STATEMENT

September 2025

1. GENERAL

This AML Policy Statement (the “Statement”) sets out a brief framework in which **B2B Prime Services Africa (Pty) Ltd** (subsidiary of B2B Prime Services EU Limited) (“B2Prime ZA”), a licensed Financial Service Provider authorised and regulated by the Financial Sector Conduct Authority of South Africa (”FSCA”) with FSP license no. 54191, complies with its Anti-Money Laundering (“AML”) and Countering the Financing of Terrorism (“CFT”) obligations.

These obligations include those espoused in the Financial Intelligence Centre Act (“FICA”), the Prevention of Organised Crime Act (“POCA”), the Prevention and Combating of Corrupt Activities Act (“PRECCA”), and international standards as set out by the Financial Action Task Force (“FATF”)

2. SCOPE OF APPLICATION

This Statement applies to all employees and representatives of B2Prime ZA, including its directors and key individuals, as well as to all of its customers of any of the services offered by B2Prime ZA.

3. GOVERNANCE, RISK AND COMPLIANCE

Compliance with regulatory requirements, prudential norms, and industry best practices not only enhance the efficiency and reputation of B2Prime ZA, but also boosts investor confidence and helps management meet stakeholders’ expectations of integrity. Adhering to laws, rules, and standards is essential, encompassing market conduct, ethical business practices, conflict management, and the fair treatment of clients and stakeholders.

For compliance to be truly effective, it must be integrated into the company culture and reinforced through a strong alignment of values, processes, and rewards. A holistic approach to compliance ensures that its benefits far outweigh the associated costs. At B2Prime ZA, we prioritize full compliance with all regulatory requirements, starting at the highest levels of the firm. Our core principles of governance and compliance include:

3.1. Maintain a strong compliance function: Responsible for assessing, monitoring, and reporting on regulatory adherence and the effectiveness of supervisory procedures.

3.2. Act professionally and ethically: Always put clients' interest first, communicate clearly, and maintain fairness and integrity.

3.3. Ensure independence and objectivity: Avoid relationships that may compromise or appear to compromise these values.

3.4. Uphold transparency and disclosure: Comply with capital market rules and regulations, in both letter and spirit.

3.5. Foster a culture of ethics and compliance: Promote high ethical standards and investor

protection.

4. RESPONSIBILITIES

4.1. Board of Directors:

4.1.1. Oversee governance and compliance, approve GRC policy, and ensure effective risk management.

4.1.2. Promote values of honesty and integrity, and ensure compliance policies are communicated and followed.

4.1.3. Appoint the Compliance Officer (CO) and ensure independent audits of ML and TF policies.

4.2. The Compliance Officer:

4.2.1. Manage the compliance function, ensure effective implementation, and advise on new business processes.

4.2.2. Address breaches, report compliance issues, ensure regulatory compliance, and provide staff training.

4.2.3. Reporting suspicious transactions to the Financial Intelligence Centre ("FIC").

4.3. All Employees:

4.3.1. Comply with all AML procedures and report suspicious transactions to the CO or MLRO.

5. RISK BASED APPROACH

A risk-based approach (RBA) is a strategic framework used in financial services and regulatory practices that focuses on identifying, assessing, and managing risks in a proportionate and prioritized manner and allows institutions to allocate resources more efficiently and focus efforts on areas that present the greatest threat. B2Prime ZA employs a risk-based approach to compliance, tailoring the intensity of monitoring and due diligence based on the risk profile of the customer or the transaction. This approach ensures resources are allocated efficiently, with higher attention given to higher-risk customers and transactions. Countries or geographic areas, products, services and transactions the clients offer or undertake, and the delivery channels by which those products, services and/or transactions are provided are all taken into account.

A risk assessment involves evaluating potential threats, their likelihood, and impact, while considering changes in activities and compliance with current legislation. Mitigation strategies include enhanced due diligence, improved reporting, and limiting business with high-risk countries. Residual risks are managed through targeted actions, with regular reviews and monitoring to adapt policies as threats evolve. Action plans are executed under compliance supervision, with ongoing follow-ups and documentation to ensure effective risk management. ti.

6. CUSTOMER DUE DILIGENCE

B2Prime ZA follows comprehensive Customer Due Diligence (CDD) measures to prevent money laundering and terrorism financing. These include verifying the identity of applicants, beneficial owners, and individuals with controlling ownership interests. If control is unclear, the senior managing official's identity is verified. The company also assesses the purpose and nature of business relationships, conducting ongoing due diligence and transaction monitoring to ensure consistency with the customer's profile. CDD information is sourced from reliable, independent data, and regularly updated, especially for high-risk clients. The company records information if a third party is involved, including their identity and relationship to the applicant. If unable to verify this, a Suspicious Transaction Report (STR) is filed. Providing false information in CDD processes is an offense, punishable by fines and imprisonment.

6.1. Politically Exposed Persons (PEPs)

PEPs are individuals who are or who have been entrusted with prominent public functions (e.g. Heads of State or of Government, Senior Politicians, Senior Government, Judicial or Military Officials, Senior Executive of State-owned Corporations and important Political Party Officials) in foreign, domestic and international organisation PEP, as well as family members and close associates of such person. Business relationships with PEPs pose a greater than normal money laundering risk to financial institutions, by virtue of the possibility for them to have benefited from proceeds of corruption, as well as the potential for PEPs (due to their offices and connections) to conceal the proceeds of corruption or other crimes.

6.2. Procedures Applicable to Foreign PEPs

6.2.1. Put in place and maintain appropriate risk management systems to determine whether the customer or beneficial owner is a PEP

6.2.2. Obtain senior management approval before establishing or continuing, for existing customers, such business relationships;

6.2.3. Obtain similar approval from senior management in cases of family members or close associates of PEPs;

6.2.4. Take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and

6.2.5. Conduct enhanced ongoing monitoring on that relationship.

6.3. Important Aspects for PEPs

6.3.1. A reporting person shall apply the relevant requirements of screening and escalation to family members or close associates of all types of PEP, as may be specified by a supervisory authority or regulatory body after consultation with the National Committee.

6.4. Suspicious Transactions

A suspicious transaction refers to any financial activity that may involve money laundering, terrorism financing, or funds linked to criminal enterprises, even if the funds themselves are not directly from illegal activities. Such transactions often occur under unusually complex, opaque, or illogical circumstances that lack a clear economic rationale or lawful purpose. Additionally, transactions conducted by parties whose identities cannot be adequately verified or those that raise any other red flags of irregularity or risk are considered suspicious. These transactions warrant further scrutiny to prevent potential criminal activities, such as fraud, corruption, or terrorism.

6.5. Suspicious Transactions Report (STR)

All employees are required to submit an STR to the Compliance Officer or the Money Laundering Reporting Officer (MLRO) when coming across a transaction, client or activity that they consider suspicious, and after further examination of the same:

6.5.1. The STR shall be passed from the CO to the MLRO.

6.5.2. The MLRO shall assess the information contained within the report to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/TF or Proliferation Financing.

6.5.3. The MLRO shall forthwith make a report to the FIC where there is reason to believe that an internal disclosure may be suspicious.

6.5.4. An internal registry should be kept for STRs that have not been submitted to the FIC.

6.5.5. The internal registry should be updated on a monthly basis, regardless of any suspicious transactions, clients or activities have been flagged or a STR being submitted.

6.5.6. An external registry should be kept for STRs that have been submitted to the FIC.

6.5.7. A maximum delay of 5 working days is required for the reporting of the STR to the FIC, after the MLRO becomes aware of a suspicious transaction or activity.

6.6. Loss of Contact with Client (PEP) or otherwise

The loss of contact with the client may occur when the client has either deceased and does not leave any alternate contacts; has moved physical address for personal or business reasons and purposely does not leave either forwarding contact details or any means of further contact or simply has been negligent in keeping up to date on his affairs.

The Client should already have been classified one of low, medium or high risk. In the event the Client is of low or medium risk it is possible that there is no contact with the client within an 11-month period.

In the event the Client is of high risk or a PEP, there should be regular contact throughout the year and review of the file because of the nature of the client. If the Client is not responding to

regular contact methods, the following steps should be taken by the Compliance Officer.

6.6.1. Original follow-up document sent with advice of delivery to the last recorded physical address on file.

6.6.2. Follow-up within a one-month period

6.6.3. During the above period, the client may be contacted. The documentation advising the client of the proceedings of the Company, including fees and other responsibilities may be delivered by the local office to the physical address of the client if known.

6.6.4. Although the client may persist in not responding to any of the contact made, a continued annual contact is to be made until such a stage as the company itself is wound up or the Board takes alternative action.

6.6.5. Should the client be unreachable within a period of one year, the Commission will be informed accordingly. The Board is to review on an annual basis all Client files where the client is no longer responding to any contact and may take further action on the Client as is deemed appropriate considering the Business Risk to the Company.