BOLDSCALE AML Policy

Last Updated: March 2024

1. Purpose

BOLDSCALE TECHNOLOGIES INC. & BOLDSCALE TECHNOLOGIES LTD. (“BOLDSCALE”, “The Company'', “We”, “Us”, “Our”) has defined this AML Policy to help prevent the use of Bonndle Super App (“Bonndle”, “The Platform'') for money laundering or terrorist financing activities. This policy outlines the measures and procedures in place to detect, prevent, and report suspicious activities.

2. Scope

To ensure compliance with applicable laws and regulations the AML Program includes the following components:

- **Customer Identification Program (CIP):** We will verify the identity of all users who open an account or engage in transactions. The CIP will include procedures for verifying the identity of individuals, entities, and beneficial owners.
- **Risk Assessment:** Risks assessments will be conducted on users and transactions to identify and mitigate potential money laundering and terrorist financing risks.
- **Monitoring and Reporting:** User activity will be monitored for suspicious transactions and where needed reported to the appropriate authorities.
- **Training and Education:** We will provide training and education to our employees and contractors on AML regulations and procedures.

3. Customer Identification Program (CIP)

The CIP will include the following procedures:

- Verification of identity: We will work with our partners to verify the identity of all users who open an account on Bonndle. This will include collecting identifying information such as name, date of birth, and government-issued identification number.
- Risk-based approach: A risk-based approach will be taken to the CIP, applying enhanced due diligence measures for higher risk users and transactions.

4. Risk Assessment

Activities to identify, prevent and address risks will include:

- Assessing the risk profile of each user based on factors such as geographic location and transaction activity.

- Identifying high-risk users and transactions and applying enhanced due diligence measures.
- Regularly reviewing and updating the risk assessment to reflect changes in the user base and transaction activity.

5. Monitoring and Reporting

This will include:

- Implementing automated monitoring systems to detect suspicious transactions.
- Investigating and reporting suspicious transactions to the appropriate authorities.
- Maintaining records of all suspicious activity reports and related documentation.

6. Training & Education

Training activities will include:

- Providing training on AML regulations and procedures.
- Providing training on identifying and reporting suspicious activity.
- Regularly updating and reviewing the training program to ensure it remains current and effective.

7. Contact Information

For further information and enquiries contact us at team@boldscale.io.

Signed

Austin Nwokediuko (CEO)