Anti-Money Laundering and Counter Terrorism Financing Policies

SCOPE OF THE POLICY

Kviku Holding Ltd. (hereinafter - Kviku) and its subsidiaries/affiliates (hereinafter Kviku Group) are subject to various anti-money laundering (AML) laws and regulations relevant to the specific business and jurisdiction where the business operates. Kviku commits to comply with applicable regulations and ensure that appropriate measures are taken to combat money laundering, terrorism financing and financial crime.

Kviku Group AML/CTF Policies applies to all employees, including those of wholly and majority-owned entities. Subsidiaries, affiliates, and business units may adopt AML/CTF policies specifying additional AML/CTF compliance requirements and procedures in accordance with applicable laws of the locations where each does business or is located.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally-derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. 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.

Terrorism financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorism financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorism financiers, the actual methods used to fund terrorism operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorism attacks does not always require large sums of money and the associated transactions may not be complex.

Kviku Group AML/CTF policies, procedures and internal controls are designed to ensure compliance with all applicable AML/CFT regulations. The policies will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

AML COMPLIANCE COMMITTEE

The AML Compliance Committee, with full responsibility for the Policy shall consist of the Company shareholders and the AML Compliance Officer. The duties of the AML

Compliance Committee with respect to the Policy shall include, but are not limited to, the drafting and implementation, as well as updating of the Policy as required; training of officers, employees; monitoring the compliance of Kviku Group subsidiaries, affiliates, and business units, maintaining necessary and appropriate records, filing of SARs (suspicious activity reports) and STRs (suspicious transaction reports); and independent testing of the operation of the Policy. Each Kviku Group 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.

KNOW YOUR CUSTOMER STANDARDS AND CUSTOMER DUE DILIGENCE

Kviku have established, documented and maintain **Know Your Customer** (KYC) and **Customer Due Diligence** (CDD) that are integral part of the Kviku Group AML/CTF Policies. They may differ under the laws of the country in which a particular group member operates.

Verifying Information

Based on the risk, and to the extent reasonable and practicable, Kviku Group will ensure that it has a reasonable belief of the true identity of its customers. In verifying customer identity, designated employees shall review photo identification. Kviku Group shall not attempt to determine whether the document that the customer has provided for identification has been validly issued. For verification purposes, Kviku Group shall rely on a government-issued identification to establish a customer's identity. Kviku Group however, will analyze the information provided to determine if there are any logical inconsistencies in the information obtained.

Records Keeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records containing a description of any document that we relied on to verify a customer’s identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all KYC information, transactions and customer`s account activities for 10 (ten) years after the account has been closed or last transaction was made.

Customers Who Refuse To Provide Information

If a customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the designated employee shall

notify their Business team. The Kviku Group Business team will decline the application and notify the AML Compliance Officer.

General Customer Due Diligence and Risk Based Approach

We pay special attention to obtaining the necessary information about customers that allows us to evaluate the risk presented by each customer and to detect and report suspicious activity. When we review a customer transaction, the due diligence we perform may be in addition to customer information obtained for purposes of our KYC.
For each transaction, we analyze risks, in the event there are circumstances in which we cannot perform appropriate due diligence, we will determine appropriate action including, but not limited to suspension of the transaction and/or closure of the customer's account. It's Kviku Group policy to mitigate the risks identified by each transaction.
Kviku Group does not work with third party accounts and cash. All payments from customers to the Group and vice versa are made through banking institutions, as well as authorized payment systems, which are guided by their own Policies when interacting with the customer.

RED FLAGS, SUSPICIOUS ACTIVITY AND SUSPICIOUS TRANSACTIONS

There are signs of suspicious activity and suspicious transactions 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:

- Suspicious Customer Behaviour:
    - overly secretive client
    - client refuses to provide information
    - client appears disinterested with outcome
    - client uses multiple bank accounts
- Suspicious Customer Identification Circumstances:
    - client provides counterfeit documents
    - client only provides copies rather than original documents
    - client only provides foreign, unverifiable identity documents
    - client only acts through a third party
- Suspicious Transactions:
    - multiple transactions in a short period of time
    - unusual source of funds
    - request for payments to third parties