

DataWave Tech Ltd – ANTI-MONEY LAUNDERING POLICY

DataWave Tech Ltd (hereinafter referred to as the “**Company**”), is a company registered with the registrar of International Business Companies in Saint Lucia with registration No. 2023-00512, authorized by the Mwali International Services Authority under an International Brokerage and Clearing House License number T2023409.

The Company does its utmost to ensure that the privacy, confidentiality and security of its clients are preserved both throughout their interaction with the Company and afterwards, to the fullest extent achievable by the Company. At the same time, the Company is obliged to follow certain requirements as set out by its applicable regulatory framework for the prevention and suppression of money laundering activities. As such, the Company is obliged to follow strict Anti-Money Laundering (AML) and Counter Terrorism Financing procedures, meaning that it is required to obtain certain verification information and documentation.

The Company determines the identity of all of its clients’ accounts and does not continue the business engagement with such accounts unless it satisfies this requirement. It has established procedures to obtain appropriate evidence of clients’ identities, and maintains adequate records of clients’ identities and transactions in such a manner so as to assist, if necessary, in the investigation of criminal offences.

The Company has policies and procedures in place to identify and avoid money laundering related transactions and to ensure compliance with the requirements of any relevant legislation issued by its regulator.

The Company is vigilant in ensuring the prevention of its involvement or misuse in money laundering activities and is not knowingly accepting assets or entering into business relationships where there is reasonable cause to believe that such assets may have been acquired illegally or may represent the proceeds of criminal activity.

The Company shall promptly report suspicious transactions relating to any account to its Supervisory Authority. Where there is suspicion that the source of funds may be criminal or that a client may be involved in criminal activity, the Company shall follow established procedures for assessing the evidence and shall determine the most appropriate course of action to be pursued.

The Company shall keep records of reports made by its staff and of reports made to its Supervisory Authority. The Company establishes the identity and verifies the identity of any client of the Company by requiring the client to provide an identification document (i.e. a passport, government issued identity card, or driving license). The Company maintains the right to request any additional documentation that might be deemed necessary at any point of the business relationship.

The Company shall:

1. obtain information on the purpose and nature of the business relationship when establishing a new business relationships;
2. adequately identify and verify the identity of any natural person when a transaction is conducted, including information relating to:

- the person's name and address;
 - the national identity card, social security document, passport or other applicable official identifying document.
3. adequately identify the beneficial owner of any legal entity conducting a transaction with the Company and take reasonable measures to identify and verify its ownership and control structure, including information relating to:
- the customer's name, legal form, head office address and identities of directors;
 - the principal owners and beneficiaries and control structure;
 - provisions regulating the power to bind the entity and to verify that any person purporting to act on behalf of the customer is so authorized, and identify those persons;
4. have appropriate risk management systems to determine if a customer or beneficial owner is a politically exposed person, and if so, shall:
- adequately identify and verify their identity as set out in this section;
 - obtain the approval of senior management before establishing a business relationship with the politically exposed person;
 - take reasonable measures to establish the source of funds and source of property; and
 - conduct regular enhanced monitoring of the business relationship.

Should you require any further information and/or have any questions about this document, please contact us at support@maunto.com.