Anti-Money Laundering Policy

1. Purpose

This policy outlines the systems and controls developed by Demerara Distillers Limited (DDL) to detect, control and reduce the risk of our services being used by criminals to launder money.

2. Scope

This policy shall apply to all companies and employees in the DDL Group as well as third parties who engage in business on behalf of DDL.

3. Commitment

DDL is committed to:

i. complying with all anti-money laundering laws in the countries in which we operate;
ii. identifying and reporting any actual or suspected instances of money laundering of which it becomes aware;
iii. educating key employees on money laundering and the financing of terrorism in order to equip them with the knowledge to be able to recognize the methods utilized by criminals to launder money.

4. What is Money laundering?

Money laundering is the illegal process of moving funds generated by a criminal activity “dirty money”, such as drug trafficking or terrorist funding, into a legitimate business and financial process, "laundering" so as to hide the criminal origin of such funds and make same appear clean.

5. Definitions:

In relation to this policy, the following definitions apply:

- “Natural person”- means a human being.
- "Legal entity”- means corporation, partnership, trust or estate, syndicate, association, Joint Stock Company, unincorporated organisation or group capable of acquiring rights and entering into obligations.

- "Beneficial owner"- means the true owner of an asset or security even though the asset or security is in another name.
- "Politically exposed person"- means any individual who is or has been entrusted with prominent public functions on behalf of a country, including the Head of State, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned corporations, important political party officials, including family members or close associates of the politically exposed person
- "Negotiatiable instrument"- means a signed document that promises a sum of payment to a specified person or entity.

6. Know Your Customer/Supplier/3rd Party - Due Diligence

6.1 At all times, DDL's internal controls and due diligence systems must ensure that there is sufficient information necessary to establish:

i. the identity of any third party attempting to conduct business with the Company; and
ii. the purpose of the intended business relationship

6.2 While each business unit and process may implement such due diligence measures as may be deemed appropriate, from time to time, given the nature of transactions, types of customers and risks involved, the following ought to be the minimum identification and verification requirements for third parties engaging the Company in financial transactions:

a. if the transaction is conducted by a natural person- adequately identify and verify the person's identity by completing the prescribed Due Diligence Form;
b. if the transaction is conducted by a legal entity- take reasonable measures to identify and verify its beneficial ownership and control structure by completing the prescribed Form;
c. if the customer or beneficial owner is a Politically Exposed Person, do all of the following:
    i. adequately identify and verify the customer's identity by completing the prescribed Form;
    ii. have appropriate risk management systems to verify that the person is a Politically Exposed Person;
    iii. obtain the approval of Senior Management before establishing a business relationship with the Politically Exposed Person;
    iv. conduct regular monitoring of such business relationship

6.3. Employees must ascertain whether a potential client/customer is based in a country which has been black listed by The Financial Action Task Force (FATF) by reviewing the most recent list of black listed countries at the relevant date on the FATF webpage http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-june-2020.html.

6.4. Employees must keep for the duration of a business relationship with a customer and for a period of at least 7 (seven) years from the date of termination of such a business relationship, records of:

i. all information obtained under 6.2;
ii. the nature and date of each business transaction;
iii. the type and amount of currency involved in each transaction;
iv. if the transaction involves a negotiable instrument, other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee, if any, the amount and date of the instrument, the number, if any of the instrument and details of any endorsements appearing on the instrument;
v. and business correspondence with the said customer/s.

7. Procedure to be followed in the case of suspicious circumstances

7.1. Where reasonable enquiries are made and an employee forms the reasonable belief that the circumstances of a transaction are suspicious, the employee must report the suspicious transaction to DDL's Legal Department which, after conducting a review of all information provided by the employee, will determine whether the transaction is, in fact, suspicious.

7.2. The Legal Officer will report any transaction deemed suspicious to the Financial Intelligence Unit.

7.3. A reported transaction will not be carried out without the consent of the Financial Intelligence Unit.

7.4. The third party will not be informed that a transaction has been reported to the Financial Intelligence Unit, as this is an offence under the Anti- Money Laundering and Countering the Financing of Terrorism Act 2009.

7.5. All documentation related to a suspicious transaction will be submitted to the Financial Intelligence Unit

8. Compliance

8.1. DDL is committed to ensuring that it makes all required disclosures to the relevant authorities in compliance with the Anti-Money Laundering and Countering the Financing of Terrorism Act and shall not commit offences under the said Act such as:

- the falsification and concealment of documents;
- or tipping off by informing third parties that their business activities have been reported to the relevant authorities.

8.2 Compliance will be continually monitored by the Legal Department through any or all of the following methods:

a. File audits

b. Reports or feedback from staff
c. Any other method

9. <u>Review</u>

- This Policy will be reviewed from time to time as DDL deems necessary as part of DDL's overall risk management process. The policy will also be reviewed if:
  i. there are changes in the law or practice;
  ii. there are changes in the nature of DDL's business or other changes which impact on this policy;
  iii. deemed necessary by the Board