Notice Gor Jor 072/2566

Regarding Policy on Anti-Money Laundering and Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing

The company's Board of Directors Meeting No. 7/2023 held on 27 July 2023 passed a resolution to revise and update the Policy on Anti-Money Laundering and Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing in order to comply with the Anti-Money Laundering Act of 1999, Ministerial Regulation on Customer Due Diligence 2020, The Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act of 2016, and guidelines of the Anti-Money Laundering Office (AMLO), plus rules and regulations related to the two Acts, both existing and future revisions. Key details as follows.

1. Policy on Anti-Money Laundering and Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing require that staff strictly comply with the policy and operating guidelines of AMLO.

   1.1 The company shall designate a management executive who shall be authorized to ensure compliance with laws regarding anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction, and to serve as contact person with AMLO.

   1.2 The company shall implement risk management controls for anti-money laundering, terrorism financing, and proliferation of mass destructions which may stem from the use of its products and services.

   1.3 The company shall support and encourage its staff to develop adequate knowledge about anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction, in order to effectively comply with laws relevant to these issues.

   1.4 The company shall establish and implement the Policy on Anti-Money Laundering and Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing. This policy and its operating guidelines shall be given high importance as follows:

      1.4.1 Produce a risk assessment and risk management report concerning money laundering, counter-terrorism financing, and proliferation of weapons of mass destruction.

      1.4.2 Evaluate and manage the risks concerning money laundering, terrorism financing, and proliferation of weapons of mass destruction on a regular basis, with emphasis on the following guidelines.

         (a) Report on the risk assessment and management in accordance with the national assessment report on anti-money laundering and counter-terrorism financing.

         (b) Assess and manage the business operating risks of the company, in consideration of the risk exposure to money laundering, terrorism financing and proliferation of weapons of mass destruction, as required by law. Emphasis are on the following.

            (1) Customer related risks

            (2) Location or country specific risks

(3) Product and services related risks

(4) Distribution channel related risks

1.4.3 Establish measures and operating procedures to mitigate risks concerning money laundering, terrorism financing, and proliferation of weapons of mass destruction.

1.4.4 Ensure data used to assess the risks of money laundering, terrorism financing, and proliferation of weapons of mass destruction are kept up to date.

1.4.5 Establish effective working procedures to cascade data of risk assessment and management of money laundering, terrorism financing, and proliferation of weapons of mass destruction to AMLO.

1.5 The company shall establish operating guidelines and operating manual that integrates Policy on Anti-Money Laundering, Terrorism Financing, and Proliferation of Weapons of Mass Destruction in the following areas.

(1) Customer on-boarding

(2) Customer due diligence

(3) Management of customer-related risks which may involve money laundering, terrorism financing, and proliferation of weapons of mass destruction.

(4) Use of IT technology and systems to assist with customer due diligence

(5) Verification processes in the customer due diligence process

(6) Reporting of suspicious activities when conducting a customer due diligence

(7) Data maintenance

2. The company shall establish secondary policies and measures on anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction as follows.

2.1 Customer on-boarding policy

The company shall require the customer to reveal his/her identity and the company shall conduct a customer due diligence before approving/rejecting the on-boarding of this person as a customer in accordance with laws regarding anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction. Work flows are described as follows.

Step 1 Obtain the customer's identity

The company shall obtain the customer's identity according to guidelines and procedures outlined by the Ministerial Regulation on transactions whereby financial institutions and professionals covered by Section 16 must obtain the customer's identity, as well as Cabinet Announcement regarding customer identification methods for financial institutions and professionals covered by Section 16. Details subjected to type of customer.

Step 2 Customer identification process

The company must obtain other additional information about the customer which could help verify the identity of the customer and determine the risk level of the customer, in order for the company to decide whether to accept or reject this potential customer. Such data may include source of income or funds used to conduct the transaction, information about a beneficiary, etc.

Step 3 Customer due diligence

- The company must review to ensure that customer identification data and documents are complete and verified. Data may be compared against other reliable sources.
- The company must check customer's name against name-list of designated persons established by the laws on anti-money laundering and terrorism financing acts, and proliferation of weapons of mass destruction.

Step 4 Acceptance or rejection of a customer

- Acceptance or rejection of a relationship / transaction with high risk customers shall be upon the consideration of a high-level staffs holding the position at the level of Vice President upwards.
- The company shall reject a customer relationship / transaction if the following occurs:

  (1) The customer's name appears on the name-list of designated persons established by the laws on anti-money laundering and terrorism financing acts, and proliferation of weapons of mass destruction.

  (2) The company did not receive important information or supporting documents to assess the customer's identity or establish his/her risk level with regards to money laundering and terrorism financing.

  (3) The customer uses a pseudo name or nominee name or provided fabricated data or presented fake documents, etc.

2.2 Risk management for money laundering, terrorism financing, and proliferation of weapons of mass destruction.

The company shall specify risk factors for each customer type and apply risk management measures for various products and services, service and transaction channels, either existing now or to be added in the future. These risk factors will provide emphasis for the risk management process.

(1) Management of internal company risks include customer-related risk factors, location and country, products and services, service distribution channels, etc.

(2) Management of customer-related risks centers on risks associated with the customer itself, location and country, products and services, service distribution channels, including the possibility of integrating other contributing factors, to assess the risk exposure level, produce a risk management report, and update the risk assessment. The company shall rank the customer's risk level into 3 tiers.

(a) Low risk

(b) Medium risk (customers that are neither low risk or high risk)

(c) High risk. When on-boarding a high-risk customer, approval must be received from a management executive that has authority.

2.3 Customer due diligence

This refers to the process to verify and review information, monitor financial transaction activities, and data on the customer on an on-going basis until the customer relationship ends.

(1) Establish procedures on how to conduct the customer due diligence which covers the characteristics and types of transactions, value of transactions, changes to customer data, including reviews of transaction/activity data and customer profile data.

(2) Define results expected to receive from the customer due diligence.

(3) Establish the customer due diligence process for a high-risk customer.

(4) Establish the customer due diligence process for electronic money transfers such as local electronic money transfers and cross-border electronic money transfers.

2.4 Staff recruitment and training

The company shall establish a staff recruitment and selection process prior to appointing that individual to handle work concerning anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction. For example, the process should include inspection of the candidate's criminal records and name-list of designated persons.

The company shall arrange training sessions for staff to strengthen their understanding about the policy and operating guidelines with regards to anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction, when staff is newly employed and also as an on-going basis over the duration of the job duty at least once a year or when related laws and regulations changed.

2.5 Internal audit

The company shall establish an internal audit independently operated by a department or staff designated for this function to inspect in-house work related to anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction. An internal audit report shall be produced to report and inform the management overseeing the company's business operations.

2.6 Improvements and revisions to the policy

The policy and operating guidelines on anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction should be reviewed on a regularly basis, at least once a year. They should be improved and revised to comply with updated rules and regulations or when there are launches of new products, services, and transaction channels involving technology which may contain risk exposure to money laundering, terrorism financing, and proliferation of weapons of mass destruction

3. Establish measures to share information with other businesses within the industry, such as account data, customer's transaction data, customer's transaction activities, analytical data, suspicious transactions or activities which may constitution money laundering, terrorism financing, or proliferation of weapons of mass destruction, or any other data which helps comply with the policy on anti-money laundering, terrorism financing, and proliferation of weapons of mass destruction, etc. This also includes measures covering data privacy and non-disclosure, as prescribed by law.

4. The Chief Executive Office shall be empowered to establish the policy and operating guidelines on anti-money laundering, terrorism financing, or proliferation of weapons of mass destruction according to the resolution of the Board of Directors, to be used as company operating guidelines. It shall be submitted to the Board of Directors for acknowledgement.

5. Repeal the earlier Notice Gor Jor 025/2564 regarding Policy on Anti-Money Laundering, Terrorism Financing, and Proliferation of Weapons of Mass Destruction dated 23 April 2022, to be replaced instead by this particular policy document.

6. This policy is effective 9 August 2023 onwards.

Notice issued 9 August 2023

(Mrs. Chavinda Hanratanakool)

Chief Executive Officer