(Translated version)

CP ALL Public Company Limited

At L&C 18/2018

Anti-money laundering policies and prevention of financial support for terrorism and the proliferation of weapons of mass destruction Policy Announcement

---

1) Principles and reasons

The company is aware of the duties and business ethics in order not to be a tool of the money laundering process, terrorism, and weapons proliferation of high destructive power which may affect the reputation and damage to the business of the company and the overall economy of the country causing unlawful business operations not in accordance with the Anti-Money Laundering and Prevention Act, BE 2542 (1999), Prevention and Suppression of Financial Support to Terrorism and the Proliferation of Weapons of Mass Destruction Act, BE 2559 (2016) and other related laws.

To prevent such damage, the company has therefore established this policy with the highest priority and must be treated strictly for the personnel of the company and any related persons to have knowledge and understanding and able to perform work or conduct transactions, assess, and manage risks that may arise from money laundering that are conducted through the company's business channels, in accordance with the law and according to international standards for anti-money laundering and preventing financial support for terrorism and the proliferation of weapons with high destructive power.

2) Objectives

2.1 To be a guideline for the operation of anti-money laundering and prevention of financial support to terrorism and the proliferation of weapons of mass destruction according to the international standards and according to the Anti-Money Laundering Act, BE 2542 (1999) and Prevention and Suppression of Financial Support to Terrorism and the Proliferation of Weapons of Mass Destruction Act, BE 2559 (2016), including any other official requirements

2.2 To allow executives, employees, and those related to the company to correctly have a good understanding and in the same direction in implementation of this policy.

2.3 To be a guideline for managing the processes and procedures within the organization about receiving customers, checking customer facts, prevention and risk management that may occur from money laundering or financial support to terrorism and the proliferation of weapons of mass destruction.

3) Scope of Application

For this announcement, it is effective with CP All Public Company Limited and its subsidiaries.

4) Definitions

"Company"	means CP ALL Public Company Limited and its subsidiaries.
"Subsidiary Companies"	means limited companies or public limited companies which are under the control of CP ALL Public Company Limited in accordance with the notification of the Securities and Exchange Commission (SEC).
"Customers"	means natural person, juristic person, or person having legal agreement which has a business relationship or a transaction with the company.
"The person who has legal agreement"	means an agreement for an individual or a juristic person to be a possessor, use, sale, or management of property in any way for the benefit of individual or juristic person of the other party.
"Money Laundering"	means the use of money or assets obtained from offenses or acquired unlawfully and change the condition into money or property that has been acquired correctly.
"Transactions"	means activities related to contractual juristic acts or any actions with others in business finance or the operation of assets.
"Suspicious transaction"	means a transaction that has reasonable grounds to believe that it has been done in order to avoid money laundering offenses or transactions that are related to or may be related to the violation of the law.

"Know your customers: KYC"	means receiving information from customers and checking the accuracy and reliability of information received from customers according to the announcement of the Office of the Prime Minister on the method of presence of customers of financial institutions and professionals under Section 16.
"Identification of customers"	means collecting information around the client's side in addition to the data from customers' presence, such as information on other sources of income of customers, information on customers' business operations, etc., in order to know whether customers are at risk of money laundering and financial support for terrorism and the proliferation of weapons of mass destruction which must refuse to build a relationship or not, along with the information that has been taken to assess the risk.
"Customer Due Diligence (CDD)"	means the process of monitoring, checking, and reviewing on customers' financial movement or transactions on a regular basis. Such processes must be consistent with the level of risk, which is evaluated based on information and various factors appropriately. With the results obtained from verification to know the facts about customers will allow the company to consider improving the risk level appropriately for the safety of the company from being a source of money laundering and financial support for terrorism and the proliferation of weapons with high destructive power.
"Professionals according to Section 16 under the Anti-Money Laundering Act, BE 2542 (1999)	means (1) professionals regarding the operation, providing advice, or being a consultant in transactions involving investment or capital movements under the law of securities and stock exchanges that are not financial institutions. (2) professionals who trade gemstones, jewels, gold, or jewelries that are decorated with gems, jewels, or gold.

(3) professionals who trade or hire-purchase cars

(4) professionals dealing with real estate brokers or agents.

(5) the antique trader under the law of auction control and the sale of antiques.

(6) professionals concerning personal loans under supervision for entrepreneurs which are non-financial businesses accordingly to the Ministry of Finance's announcement regarding assembly personal loan business under supervision or according to the law on financial institutional business.

(7) professionals concerning non-financial electronic money cards according to the notification of the Ministry of Finance regarding the operation of electronic money card business or under the law on financial institution business.

(8) professionals related to credit cards that are not financial institutions as announced by Ministry of Finance regarding credit card business or according to the law of financial institution business.

(9) professionals relating electronic payments under the law on supervision of electronic payment services business.

(10) professionals who conduct financial business under the law on money exchange control that is not a financial institution which appears from the evaluation results of risks related to money laundering or financial support to terrorism whether there are risks that may be used as a means of money laundering or financial support to terrorism or not as determined by the Ministry.

"Designated Person" means a person, a group of persons, a juristic person, or an organization according to the name of the resolution or announcement under the United Nations Security Council determined to be a person with Acts of terrorism or the proliferation of weapons of mass destruction, and the office has announced that name of person, committee, juristic person, or organization according to the list that the court has considered and ordered to be the person designated by the Anti-Money

	Laundering and Prevention Act, BE 2542 (1999) and Prevention and Suppression of Financial Support to Terrorism and the Proliferation of Weapons of Mass Destruction Act, BE 2559 (2016).
"AMLO Office"	means the Anti-Money Laundering Office.

5) Duties and responsibilities in compliance with the policy

5.1 Board of Directors is responsible for considering and approving the anti-money laundering policy and preventing financial support for terrorism and the proliferation of weapons with high destructive power.

5.2 The management team has the following duties:

5.2.1 Define measures to control and manage money laundering risks and financial support for terrorism and the proliferation of weapons of mass destruction that may arise from the use of transaction channels, products, or various services of the company.

5.2.2 Define secondary policies, orders, regulations, and internal practices that are consistent with the protection policy of anti-money laundering and the prevention of financial support for terrorism and the proliferation weapons of mass destruction according to the guidelines specified by the Office of the AMLO or any other relevant laws.

5.2.3 Determine executives with authority and duty to consider and use discretion and approve the operating procedures in both normal cases and in the case with special screening in the process of receiving customers, risk assessment, and examination to know the facts about customers.

5.2.4 Sufficiently support and encourage employees to have knowledge and understanding about anti-money laundering and the prevention of financial support to terrorism and the proliferation weapons of mass destruction to be able to effectively work in receiving customers, risk assessment, and the examination to know the facts about customers.

5.3 The regulatory compliance agency has a duty to control and supervise the operation to be in accordance with anti-money laundering policy and prevention of financial support for terrorism and the

proliferation of weapons with high destructive power and according to the Anti-Money Laundering Act BE 2542 (1999) and Prevention and Suppression of Financial Support for Terrorism and the Proliferation of Weapons of Mass Destruction Act BE 2559 (2016) and other associated official regulations including coordinating with AMLO or other agencies that have legal authority.

5.4 The internal audit unit is responsible for regularly reviewing compliance with laws annually.

5.5 Executives and employees at all levels have a duty to strictly comply with the orders, regulations, and / or guidelines set by the company under the anti-money laundering policy and to prevent financial support for terrorism and the proliferation of weapons of mass destruction.

6) Risk Management

6.1 Provide assessment and level of risk for each customer to collect data and evidence of identity to suit the level of risk.

6.2 In assessing risks, take into account the risk factors that arise from customers such as shareholder structure, list of name or occupation notified by the AMLO with a high risk, status of political persons, risk factors arising from the area or country in which the Office of the AMLO declares, including other factors such as service channels, types of transactions, types of financial products, information on names that are at risk from other sources, etc.

6.3 Requiring senior management of the company to consider approving the creation of business relationships with high-risk customers and approve the result of the review of the information in accordance with the audit process to know the facts about the customer.

6.4 The company must refuse to establish a business relationship or not make a transaction or terminate a business relationship with a customer with a high risk that may cause the company to be used as a money laundering or financial support tool for terrorism and the proliferation of weapons of mass destruction.

6.5 Provide procedures for knowing the identity of the customer (Know Your Customer: KYC) and the process of checking for Customer Due Diligence: CDD according to the risk level.

6.5.1 In the case of customers having a low risk level can consider identifying the customer from the presence information without needing to request other information.

6.5.2 In the case of customers having a high level of risk need to consider additional identification procedures by requesting information or checking other customers' information, such as utility payment information from the address or the establishment, a copy of business contract or business agreement between the customer and the third party, only the part that proves the business operation received from the customer or any reference information showing that the customer has a business relationship with a credible financial institution, etc.

6.6 The company must manage risk continuously with a follow-up process from the procedure of building relationships with customers and must proceed throughout the period until the relationship with the customer is terminated.

6.7 Subsidiaries are able to determine the acceptable risk (Risk Appetite) for proper risk management. However, the assessment and risk management must be of a standard not less than this policy and in accordance with the law.

7) Accepting customers

The company must provide measures to know the identity of the customer (Know Your Customer: KYC) by arranging for customers to show themselves, identify themselves, and conduct Customer Due Diligence checks (CDD) as follows.

7.1 Know your customers: KYC

7.1.1 The company must arrange for customers to show themselves every time before making a transaction in accordance with the rules and procedures in the Ministerial Regulations defining transactions that financial institutions and professionals in accordance with Section 16 must show themselves BE 2559 (2016) and the announcement of the Office of the Prime Minister. However, such measures must not be an obstacle in the presence of people with disabilities.

7.1.2 Arrange for customers to specify the last beneficiary name and the person who has control over the final transaction (if any).

7.2 Identification of customers

The company must check the information and documents of the client's identity in order to know the fact that customers Existed in real life according to the law and the information that the presence is sufficient for risk management and check to know the facts about customers.

7.3 Customer Due Diligence: CDD

7.3.1. Provide the factual examination of the customer or the actual beneficiary of the customer by using documents, data or information from reliable public sources other than customer information.

7.3.2. To verify the completeness of information or evidence of identity with the list of "designated person" which is a list of individuals, juristic, entities or organizations that have a resolution or announcement under the United Nations Security Council determined to be a person who has acts of terrorism or the proliferation of weapons with high destructive power or persons whose court orders as designated person.

7.3.3. In the case of a juristic person, use the information that can prove the status and existence of the juristic person, list of persons with controlling power, and supervision, including senior management of that juristic person to conduct verification in accordance with 7.3.2.

7.3.4. Clearly verify the source of assets and funds of customers before starting the transaction.

7.3.5. Examine and review customer information for a specified period of time, except in the event of a change in the transaction, a doubt about the identity of the customer or beneficiary, or a doubt about money laundering or financial support for terrorism and proliferation of weapons of mass destruction.

7.4 Approval or rejection of accepting customers

The company must refuse to establish business relationships or transactions with customers if there is an appearing fact of the following.

7.4.1. The client conceals name or real last name and surname or use alias or fake name in the transaction.

7.4.2. Customers report false information or show false evidence.

7.4.3. Use of information and proof of identity which are not in accordance with the announcement of the Prime Minister's Office on the method of presence of customers, financial institutions, and professionals under Section 16.

7.4.4. Unable to verify the identity and evidence.

7.4.5. Verifying that customers or the real beneficiary of the customer is on the list of designated persons according to the announcement of the AMLO.

7.4.6. Receiving that customer will cause the company to be exposed to money laundering or financial support for terrorism and proliferation of weapons of mass destruction.

8) Maintaining information and documents

8.1 The company requires the responsible agency to keep the information and documents related to customer transactions and internal operations of the company in a secure location or database with limited access to only relevant persons. However, the information and documents must be ready if there is a call from the AMLO Office, and the storage period is as follows.

8.1.1. Keep the identity documents for 5 years from the date of closing or terminating the relationship with the customer.

8.1.2. Collect documents of transaction and record of the facts for 5 years from the date of transaction or record of facts.

8.1.3. Keep inspection documents to know the facts of customers, such as information on other sources of income of customers, spouse information, information on the form of business operations of customers, etc. for 10 years from the date of closing accounts or terminating relationships with customers.

8.2 No person shall disclose information or act in any way that may cause customers or third parties to know about the investigation in order to know the facts of the customer and about reporting transactions or submitting any other information to the Office of the AMLO unless it is a legal action or a court order.

9) Training

The company provides training on money laundering prevention and prevention of financial support for terrorism and proliferation of weapons of mass destruction as part of the business ethics program to executives and employees.

10) Reviewing Policy

The company will review this policy at least once a year or if there is a change in the law.

11) The compliance of related subsidiaries with laws relating to the Anti-Money Laundering and Prevention Act, BE 2542 (1999), Prevention and Suppression of Financial Support to Terrorism and the Proliferation of Weapons of Mass Destruction Act, BE 2559 (2016)

Stipulates that a subsidiary who is a professional under Section 16 of the Anti-Money Laundering Act BE 2542 (1999), issued a policy to prevent money laundering and prevent financial support for terrorism and the proliferation of weapons of mass destruction including secondary policies, regulations, procedures of operations including secondary policies, regulations and procedures for the subsidiaries. However, it must not be contrary to or define policies and measures less than this policy and shall be in accordance with the Anti-Money Laundering and Prevention Act, BE 2542 (1999) and Prevention and Suppression of Financial Support for Terrorism and the Proliferation of Weapons of Mass Destruction Act BE 2559 (2016) including other relevant regulations.

Effective from 1 September, 2018 onwards.

Announced on 31 August, 2018

Mr. Korsak Chairasmisak

Chairman of Executive Committee