Anti-money laundering and counter-terrorism and the proliferation of weapons of mass destruction Policies and Procedures

Srisawad Capital 1969 Public Company Limited

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Policy and Procedures

Anti-Money Laundering and Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing of Srisawad Capital 1969 Public Company Limited

Principle

Srisawad Capital 1969 Public Company Limited ("the Company") is considered a professional profession under Section 16 (6) of the Anti-Money Laundering Act, B.E. 2542 (1999). The Company supports and is ready to conduct its business operations in compliance with the laws, regulations, and rules of the Anti-Money Laundering Office (AMLO) and other government agencies, in order to prevent itself from being used as a channel or an instrument for money laundering, or terrorism financing, and the proliferation of weapons of mass destruction, by strictly complying with the laws and guidelines prescribed by AMLO. In this regard, this Anti-Money Laundering and Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing : AML/CTPF Policy has been established, which has been endorsed and approved by the highest authorized management. This policy is deemed a core corporate policy and carries equivalent importance to the core business operation policies. Therefore, all management and employees involved in law compliance must strictly adhere to this policy.

Objective

The Company prioritizes compliance with the anti-money laundering laws and the laws governing the counter-terrorism and proliferation of weapons of mass destruction financing, so that the management and employees of the Company can conduct business correctly in accordance with the principles of the Anti-Money Laundering Act, B.E. 2542 (1999) and its amendments, including relevant subordinate legislation. This policy consists of the following key essences:

1. Customer Acceptance Policy and Procedures

In establishing or refusing to establish a business relationship with customers, the Company shall require customers to self-declare, identify, and verify the customer's identity. This process shall be conducted in accordance with relevant laws and regulations, and guidelines shall be provided to ensure that personnel can operate as required by law.

2. Risk Management Policy and Procedures

The Company defines the principles for risk management regarding money laundering, terrorism financing, and the proliferation of weapons of mass destruction financing as follows:

(1) Policy and procedures for assessing and managing risks of money laundering, terrorism financing, and the proliferation of weapons of mass destruction financing within the Company's organization. Criteria

and risk factors shall be determined in accordance with the law, and guidelines shall be provided to ensure that personnel can operate as required by law.

(2) Customer risk management policy and procedures. The Company shall determine criteria and risk factors in accordance with the law and shall manage risks throughout the duration of the business relationship with customers until the termination of the relationship, and guidelines shall be provided to ensure that personnel can operate as required by law.

(3) Policy and procedures for risk assessment of all products, services, and service channels of the Company. Criteria and risk factors shall be determined in accordance with the law. In the event of launching new products or services, developing new products and business methods, introducing new delivery mechanisms, or utilizing new or developing technologies for both new and pre-existing products, the Company shall assess and mitigate risks of money laundering, terrorism financing, and the proliferation of weapons of mass destruction financing that may arise from such new products or services developments prior to offering new products, new services, or implementing new technologies.

3. The Company requires that employees must possess knowledge and understanding of the laws governing anti-money laundering, counter-terrorism and proliferation of weapons of mass destruction financing prior to commencing work, and mandates that employees must continuously undergo training on anti-money laundering, counter-terrorism and proliferation of weapons of mass destruction financing.

4. The Company establishes measures for information sharing between the Company and its branches or affiliates, strictly prohibiting directors, executives, employees, staff, agents, or any persons of the Company, its branches, or its affiliates from disclosing information, facts, or perform any act that may cause customers or third parties to become aware of the Customer Due Diligence (CDD), transaction reporting, or the submission of any other information to the Anti-Money Laundering Office (AMLO), except in compliance with the law or a court order.

5. The Company requires transaction reporting to be conducted in accordance with the forms, criteria, and procedures prescribed by law.

6. The Company requires internal audits regarding its operating systems and compliance with the laws governing anti-money laundering, counter-terrorism and proliferation of weapons of mass destruction financing.

7. The Company requires the retention of detailed information regarding customer identification, Customer Due Diligence (CDD), transactions, and factual records of transactions for the period prescribed by law.

8. The Company establishes a plan for developing and updating policies, including manuals, to be consistent with the laws in force, which shall be reviewed and updated at least once a year or when there are changes in the law.

Definitions

"**Money Laundering (ML)**" means the conversion or transfer of money or assets derived from the commission of an offense or unlawfully acquired, into money or assets that appear to be legally acquired.

"**Terrorism and Proliferation of Weapon of Mass Destruction Financing (TPF)**" means any person who provides, collects, or conducts any financial or asset operations, or acts by any means for terrorism, knowing that the beneficiary of such financial or asset operations is a designated person, with the intention that the money or assets be used to support any activities of designated persons, individuals, groups of persons, juristic persons, or organizations associated with terrorism.

"**Customer**" means an individual person, juristic person, or a legal arrangement that establishes a business relationship or conducts occasional transactions with the Company.

"**Legal Arrangement**" means an individual person or juristic person on one part who enters into a legal agreement to possess, use, dispose of, or manage assets by any means for the benefit of another individual person or juristic person.

"**Ultimate Beneficial Owner (UBO)**" means an individual person who is the true owner or has ultimate control over the business relationship of the customer with the Company, or the person on whose behalf a transaction is being conducted, including persons who exercise ultimate effective control over a juristic person or a legal arrangement.

"**Designated Person**" means a person, a group of persons, a juristic person, or an organization on the list designated by a resolution of or an announcement under the United Nations Security Council as a person committing acts of terrorism or the proliferation of weapons of mass destruction, and whose list has been announced by the Office; or a person, a group of persons, a juristic person, or an organization on the list considered and ordered by the court to be a designated person.

"**Politically Exposed Person (PEP)**" means a person who holds or has held a prominent position in the country or a foreign country, namely a head of state or government, minister, high-ranking government official, court, independent organ, prosecutorial organ, or military; a high-ranking official of a state enterprise or other government agency; a person with a significant role in a political party; a person who holds or has held a prominent position in an international organization; and a person holding an equivalent position to such levels, as announced by the Secretary-General with the approval of the Board.

"**Family Member**" means:

(1) A father, mother, child, adoptive parent, or adopted child of a politically exposed person.

(2) A full sibling, half-sibling on the father's side, or half-sibling on the mother's side of a politically exposed person.

(3) A spouse or a person cohabiting as husband and wife without marriage registration of a politically exposed person or of a person under (1) or (2).

"**Close Associate**" means:

(1) A person who possesses or takes care of assets or any other benefits of a politically exposed person.

(2) A person who has a close relationship arising from the establishment or conduct of a business relationship with a politically exposed person.

"**Senior Management**" means a person who has the authority and responsibility for planning, directing, or controlling activities, including the management and administration of the Company.

"**Transaction**" means an activity related to entering into a juristic act, contract, or any operation with others financially, commercially, or operations concerning assets, and shall include transactions continuing from the establishment of a relationship, and transactions conducted at any one time by an occasional customer.

"**Business Relationship**" means the conduct of transactions between a customer on one part and the Company on the other part, with the objective of utilizing financial, business, commercial, or professional services of the Company on a continuous basis or during an agreed period of time.

"**Occasional Transaction**" means a transaction conducted between a customer on one part and the Company on the other part, with the objective of utilizing financial, business, commercial, or professional services of the Company on a one-off basis without the intention of establishing a business relationship with each other.

"**Suspicious Transaction (Suspicious Transaction Reporting: STR)**" means a transaction where there is a reasonable ground to believe that it is conducted in order to avoid the application of the Anti-Money Laundering Act, or a transaction connected or potentially connected with the commission of a predicate offense or terrorism financing, regardless of whether it is a single transaction or multiple transactions, and shall also include an attempted transaction.

"**Signature**" means the name of a person written by that person on a letter or document to certify or indicate that they are the maker of that letter or document, or a fingerprint and mark affixed by a person in place of their signature and shall include an electronic signature under the law on electronic transactions.

"**Reliable Source**" means a data source that provides or compiles information reasonably, systematically, or with references, enabling the public or business groups to verify or obtain various information.

"Know Your Customer (KYC)" means the process of obtaining customer identification information and verifying the accuracy and authenticity of such identification information in accordance with the Notification of the Prime Minister's Office Re: Means of Customer Identification for Financial Institutions and Professions under Section 16.

"Customer Due Diligence (CDD)" means a process established upon entering into a business relationship with a customer whose transactions reach the threshold prescribed by law, by identifying and verifying the customer's identity, identifying the ultimate beneficial owner, and monitoring the financial movement of the customer's transactions to detect whether there are any unusual circumstances or reasonable grounds for suspicion, in order to prevent the Company from being used as a channel for money laundering and/or terrorism financing.

"Risk" means the risk of money laundering, terrorism financing, or the proliferation of weapons of mass destruction financing.

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Policy and Procedures for Institutional Money Laundering, Terrorism Financing, or Proliferation of Weapon of Mass Destruction Financing Risk Assessment, Management, and Mitigation of Srisawad Capital 1969 Public Company Limited

The Company establishes the policy and procedures for assessing, managing, and mitigating the risks of money laundering, terrorism financing, or the proliferation of weapons of mass destruction financing within the organization, for strict compliance by the Company's officers. A plan is also defined to update this policy and procedures to ensure consistency and currency at least once a year, or immediately upon amendments to the law.

In this regard, the Company establishes measures related to anti-money laundering, counter-terrorism and proliferation of weapons of mass destruction financing, by incorporating risk factors regarding: 1) all customers in overall profile, 2) whether the locations or countries of business premises/affiliates/agents/branches are situated in high-risk areas, 3) products or services, 4) overall nature of transactions and delivery channels, and 5) all the adoption of risk assessment and management results from the National Risk Assessment (NRA) report compiled by AMLO, to consider for the institutional risk assessment as follows:

1) **Customer-related risk factors**: If any customer possesses the following characteristics, they may be classified as a high-risk customer for money laundering:
   1.1) The customer is a domestic or international Politically Exposed Person (PEP), or a family member or close associate of such person (examples of politically exposed persons are presented in the Appendix).
   1.2) The customer is a high-risk individual matching data notified by the Office which warrants close monitoring, where data can be verified from asset seizure or freezing orders of AMLO at: 1) the AMLO website www.amlo.go.th and 2) the AMLO Person Screening System (APS) for high-risk money laundering individuals and designated persons.
   1.3) The customer operates a cash-intensive business.
   1.4) The customer acquires cash, or operates a business involving the purchase, sale, or exchange of high-value goods, without clear sources of cash or goods.
   1.5) The customer does not engage in business operations but conducts activities resulting in the acquisition of cash or assets without a clear source.
   1.6) The customer has a residence, whether temporary or permanent, or has a source of income, or conducts transactions in areas or countries with high risks as assessed or designated by

international organizations or international bodies, such as the Financial Action Task Force (FATF), and as prescribed by the Notification of the Anti-Money Laundering Office (AMLO).

1.7) The customer is a non-resident.

1.8) The customer may be involved in a predicate offense.

1.9) The customer's business relationship or occasional transaction is conducted unusually.

1.10) The customer is a company whose shareholding structure is unusual or complex beyond standard business operations.

1.11) The customer is a juristic person in the type of a limited company that issues bearer shares.

1.12) The customer is a juristic person with nominee partners or nominee shareholders (Nominee Shareholders).

Evaluation Criteria

1. If the risk assessment results of all the Company's customers indicate low risk for more than 50 percent of the total customers, the customer-related risk factor shall be considered low risk.
2. If the risk assessment results of all the Company's customers indicate medium risk for more than 25 percent of the total customers, the customer-related risk factor shall be considered medium risk.
3. If the risk assessment results of all the Company's customers indicate high risk for more than 25 percent of the total customers, the customer-related risk factor shall be considered high risk.

2) **Geographic or country risk factors**: If the business premises, affiliates, agents, branches, service areas, or the organization's sources of income are located in the following areas, they shall be considered areas or countries with a high risk of money laundering, and the Company shall perform Customer Due Diligence at the highest enhanced level:

2.1) Areas or countries assessed or designated by international organizations or international bodies, such as the Financial Action Task Force (FATF), as areas or countries that lack measures or fail to implement or apply international standards on anti-money laundering and combating the financing of terrorism adequately (where data can be verified from the details announced on the website www.amlo.go.th -> International Cooperation on AML/CFT -> High-Risk Countries List or amlo.go.th

2.2) Areas that the Anti-Money Laundering Office (AMLO) considers as high-risk areas for money laundering or terrorism financing, including the proliferation of weapons of mass destruction financing or predicate offenses as announced and prescribed by AMLO.

2.3) Areas or countries that are sanctioned, subjected to enforcement measures, or embargoed from international trade by international organizations.

2.4) Areas or countries assessed by international organizations, international bodies, or reliable sources to have a very high rate of corruption or serious crime commission.

2.5) Areas or countries assessed by international organizations, international bodies, or reliable sources to be sources of terrorism financing, terrorist safe havens, or where terrorist organizations operate.

2.6) Areas under the declaration of an emergency situation pursuant to the law on public administration in emergency situations, such as Narathiwat Province (except Su-ngai Kolok Province, Si Sakhon District, Sukhirin District), Yala Province (except Betong District), and Pattani Province (except Mae Lan District, Mai Kaen District).

2.7) Democratic People's Republic of Korea (North Korea).

2.8) Islamic Republic of Iran.

3) **Product or Service Risk Factors**

If any of the following characteristics are met, it shall be considered a product or service with a high risk of money laundering:

3.1) A product or service that can provide, receive, or convert into cash in high value.

3.2) A product or service characterized by the transfer of monetary value that does not require identification of the transferor or the transferee.

3.3) A product or service involving anonymous transactions.

3.4) A product or service that can be transferred or change hands to other persons rapidly or conveniently.

3.5) A product or service that can be used or applied in foreign countries.

4) **Delivery Channel Risk Factors**

Delivery Channels mean the methods used by the Company to conduct transactions with customers.

4.1) **Face-to-face,** such as delivery channels through the Company's employees or the Company's agents, is considered low risk.

4.2) **Non-face-to-face,** such as delivery channels through electronic systems, is considered high risk.

5) **Risk Assessment and Management Results under the National Risk Assessment Report compiled by AMLO**, which can be viewed at www.amlo.go.th -> Topic “International Cooperation on AML/CFT” -> Topic “Money Laundering and Terrorism Financing Risk Assessment” -> Topic “National Risk Assessment Results”

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

In this regard, each institutional risk assessment and management of the Company shall utilize up-to-date data to ensure that the risk assessment and management results are accurate and complete. After performing risk assessment and risk management, appropriate risk mitigation measures and methods regarding money laundering, terrorism financing, and the proliferation of weapons of mass destruction financing shall be defined to suit the risks of each product, service, and delivery channel. If the Anti-Money Laundering Office (AMLO) requests the institutional risk assessment and management results regarding money laundering and terrorism financing, the Company shall immediately submit them to AMLO.

Customer Acceptance Policies and Procedures

Step 1 Screening Customer Names Against Designated Persons List

Prior to conducting any transaction, the Company shall screen the names of customers, beneficial owners, directors (in the case of a legal entity), and authorized persons (if any) against the Designated Persons List pursuant to the laws on Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing of Weapons of Mass Destruction. If no match is found during the screening process, personnel may proceed with the transaction. However, if a customer is identified as a designated person, the transaction shall be rejected. In the case of an existing customer who is subsequently identified as a designated person, the Company shall prepare and submit a Suspicious Transaction Report (STR) to the AMLO Office within seven (7) days. In addition, the Company shall notify the AMLO Office of the customer's designated person status within ten (10) working days from the date on which the Company becomes aware of such status, using Form PKR.04.

Step 2 Customer Identification Procedures

Personnel shall identify customers prior to every transaction, taking into account the risks of money laundering, terrorist financing, and proliferation of weapons of mass destruction of the financial products or services that establish a business relationship or occasional transaction, as prescribed in the Ministerial Regulation on Customer Due Diligence, B.E. 2563 (2020), in order to obtain the following information:

1. Individual Person

No.	Identification Information Required	Non-Low Risk Product (Medium or High Risk)	Low Risk Product	Explanation
1	Name - Surname	✓	✓	-
2	Date of Birth	✓	✓	-
3	• National Identification Number Passport number or identification number issued by the government or state agency of nationality, or identification number in an official identification document issued by the Thai government (in the case of an alien)	✓	✓	Official identification documents issued by the Thai government, such as a Work Permit, International Driving License, or Non-Thai Identification Card issued by the Ministry of Labour, etc.
4	• Address as appeared on the National Identification Card or	✓	✓	If the current address differs from the address on the identification card or

No.	Identification Information Required	Non-Low Risk Product (Medium or High Risk)	Low Risk Product	Explanation
	address as appeared on the House Registration, and current address • **In the case of** an alien, state the name of the country of nationality and current address in Thailand • **Except** for an alien who does not reside in Thailand, the current address shall be used.			house registration, both locations must be specified; however, if they are identical, it should be recorded that they are the same address.
5	Contact information, such as telephone number, electronic mail address, Line ID, or Facebook, etc.	✓	✓	-
6	• Evidence of National Identification Number • Evidence of passport number or identification number issued by the government or state agency of nationality, or identification number in an official identification document issued by the Thai government (in the case of an alien)	✓	-	Such evidence may be retained as a hard copy or as an electronic file, such as a photograph, or by extracting data from the card's storage unit (IC Chip/ NFC).
7	7.1 Occupational information 7.2 Name of workplace 7.3 Location/address of workplace	✓	-	• Specify the occupation, details, or position clearly, such as Doctor at... Hospital, Business Owner of... Company, Employee of... Company, Farmer (growing...), Police Officer..., Government Official attached to..., etc. • If the customer does not engage in any occupation (living on inheritance, or has a dependent caregiver, such as a housewife taking care of children) or

No.	Identification Information Required	Non-Low Risk Product (Medium or High Risk)	Low Risk Product	Explanation
				engages in an occupation without a permanent place of business, the address on the house registration or the current address may be used as the workplace address mutatis mutandis. • In the case of students, both the address on the house registration and the educational institution may be specified.
8	Signature of the person conducting the transaction	✓	-	• The person conducting the transaction shall sign in writing on the document or instrument, or • Provide a photograph of the signature of the person conducting the transaction, or • Provide a fingerprint or mark affixed by the person conducting the transaction in lieu of a signature, or • The person conducting the transaction shall provide an electronic signature pursuant to the law on electronic transactions.

2. **Legal Entity : Identification information must be obtained as follows:**

2.1. Name of the legal entity

2.2. Business type and business objectives

2.3. Location address and telephone number

2.4. Tax Identification Number, if any

2.5. Full name of the authorized signatory on behalf of the juristic person

2.6. Information of the ultimate authorized person designated to establish a business relationship or conduct transactions with the Company, which includes:

2.6.1. Name – Surname

2.6.2. Date of Birth

2.6.3. National Identification Number: in the case of an alien, state the passport number or identification number issued by the government or state agency of nationality, or identification number in an official identification document issued by the Thai government

2.6.4. Address as appeared on the National Identification Card or address as appeared on the House Registration, and current address; in the case of an alien, state the name of the country of nationality and current address in Thailand, except for an alien who does not reside in Thailand, the current address shall be used

2.6.5. Signature of the ultimate authorized person

2.7. Reliable evidence certifying the status of the legal entity or legal arrangement

2.7.1. Corporate customer in general: Request a Certificate of Incorporation issued by the Registrar not exceeding six months; in the case of a non-Thai registered legal entity, request evidence of legal entity status certified or issued by a reliable agency or organization not exceeding six months

2.7.2. Customers who are a government agency, government organization, state enterprise, or other state agency that is a legal entity: Request a letter of intent to conduct transactions, letter of appointment, or power of attorney

2.7.3. Customer who is a cooperative, foundation, association, club, temple, mosque, shrine, and other legal entities of a similar nature: Request a letter of intent to conduct transactions, certificate of registration from the relevant authority, letter of appointment, or power of attorney

In this regard, upon obtaining the specified identification information, measures shall be implemented to verify the customer's identity, in order to verify the correctness, authenticity, and currency of the information and supporting documents for customer identification in accordance with the following guidelines:

A. Verification of identity and review of data completeness means verifying the correctness, authenticity, and currency of identification data and evidence obtained from the identification or identity establishment of the customer from reliable data sources, as well as verifying that the customer is the actual owner

of such data and evidence, such as checking that the customer's face matches the photograph on the National Identification Card, the National Identification Card has not expired, and the customer has provided all required identification information, etc.

B. Review of supplementary data that should be available, for the purpose of contacting the customer for additional information, including information that the customer may possess but has not fully disclosed, such as a convenient contact location other than the registered address on the house registration, or a place of business other than the location specified in the registration certificate as the case may be, a secondary occupation or supplementary occupation, or a telephone number that may exceed one number, etc.

C. Verification of the correctness of data and evidence is divided into 2 categories as follows:

1) Verification of data correctness means all customer identification data must be checked to ensure that the data provided by the customer has been accurately recorded or specified in accordance with the facts notified.

2) Verification of evidence correctness means the evidence required by law for the customer to produce to the reporting entity, which includes evidence certifying the actual existence or legal status of the customer issued by a government authority or a reliable organization.

Step 3 Identification and Verification of Identity

1) In the case where the company's products or services are high risk:

The Company must identify and verify the identity of the customer based on complete identification data and obtain other information as prescribed in the Ministerial Regulation on Customer Due Diligence, B.E. 2563 (2020), and must proceed to verify the correctness, authenticity, and currency of the identification data and evidence obtained from the identification or identity establishment of the customer from reliable data sources, including verifying that the customer is the actual owner of such data and evidence, by implementing at least the following actions:

1.1) Verification of the customer's identity through face-to-face interaction.

1.1.1) In the case of using a multi-purpose National Identification Card (Smart Card) as evidence of identification, verify the data from a multi-purpose National Identification Card reader (Smart Card Reader) via the electronic verification system of a government agency, or utilize any other method with an equivalent level of reliability.

1.1.2) In the case of using a passport as evidence of identification, extract electronic data obtained from the passport, such as data from Near Field Communication (NFC) technology, to verify against the data on the passport, and inspect other official identification documents issued by the Thai government or state agencies of the country of nationality, such as a Certificate of Alien Registration

or a state-issued social security card, etc., or utilize any other method with an equivalent level of reliability.

1.2) For non-face-to-face customer identity verification, the Company shall take and record photographs of the customer and utilize advanced technology meeting international or generally accepted standards to verify and compare the customer's facial image with biometric data from a multi-purpose National Identification Card or electronic data obtained from a passport, in order to prove the true identity of that customer instead of face-to-face interactions, or utilize any other method with an equivalent level of reliability, and retain a copy of the front and back of the multi-purpose National Identification Card (Smart Card) showing a clear identification number and/or a copy of the customer's passport as evidence.

1.2.1) In the case of using a multi-purpose National Identification Card (Smart Card) as evidence of identity, the information from a multi-purpose National Identification Card reader (Smart Card Reader) must be verified through the electronic verification system of the government agency or using any other method that is equivalent to the reliability.

1.2.2) In the case of using a passport as evidence of identity. Electronic data obtained from the passport, such as information from Near Field Communication (NFC) technology, to verify against the information on the passport, and check other official identification documents issued by the Thai government or government agencies of the country of nationality, such as alien registration certificates or social security cards issued by the state, etc., or use any other method with an equivalent level of reliability

1.3) Verification of identity in the case where the customer is a legal entity: The Company shall identify and verify the identity of the customer based on complete identification data and obtain other information as prescribed in the Ministerial Regulation on Customer Due Diligence, B.E. 2563 (2020), and must verify the data and evidence against databases of government agencies by implementing the following actions:

1.3.1) Corporate customer registered in Thailand: Verify the Certificate of Incorporation issued by the Registrar not exceeding six months.

1.3.2) In the case of a non-Thai registered legal entity: Verify evidence of legal entity status certified or issued by a reliable agency or organization not exceeding six months.

1.3.3) In the case where the customer is a government agency, government organization, state enterprise, or other state agency that is a legal entity: Verify the letter of intent to conduct transactions, letter of appointment, or power of attorney.

1.3.4) In the case where the customer is a cooperative, foundation, association, club, temple, mosque, shrine, and other legal entities of a similar nature: Verify the letter of intent to conduct transactions, certificate of registration from the relevant authority, letter of appointment, or power of attorney.

2) <u>In the case where the company's products or services are medium risk:</u>

The Company shall identify and verify the identity of the customer based on complete identification data and obtain other information as prescribed in the Ministerial Regulation on Customer Due Diligence, B.E.2563 (2020), and shall proceed to verify the correctness, authenticity, and currency of the identification data and evidence obtained from the customer against reliable data sources, including verifying that the customer is the actual owner of such data and evidence, and shall implement at least the following actions:

2.1) Verification of the customer's identity through face-to-face interaction

2.1.1) In the case of using a multi-purpose National Identification Card (Smart Card) as evidence of identity, any one of the following methods may be utilized:

2.1.1.1) Verify the data from a multi-purpose National Identification Card reader (Smart Card Reader) and verify the status of the National Identification Card via the electronic verification system of a government agency, or

2.1.1.2) Verify the data from a multi-purpose National Identification Card reader(Smart Card Reader) against the data on the customer's National Identification Card, or

2.1.1.3) Verify the data on the multi-purpose National Identification Card (Smart Card) and verify the status of the National Identification Card via the electronic verification system of a government agency.

2.1.1.4) Verify the data against any other database of a government agency.

2.1.2) In the case of using a passport as evidence of identification, electronic data obtained from the passport, such as data from Near Field Communication (NFC) technology, to verify against the data on the passport; if the electronic data obtained from the passport cannot be verified, other official identification documents issued by the Thai government or state agencies of the country of nationality may be inspected as a substitute, such as a Certificate of Alien Registration or a state-issued social security card, etc.

2.1.3) Any other method with an equivalent level of reliability, or consideration may be given to utilizing biometric comparison technology to enhance the efficiency of customer identity verification.

2.2) For non-face-to-face customer identity verification, the Company shall take and record photographs of the customer and utilize advanced technology meeting international or generally accepted standards, or have personnel verify and compare the customer's facial image with the customer's image on the multi-purpose National Identification Card or passport, in order to prove the actual identity of that

customer in lieu of face-to-face interaction, or utilize any other method with an equivalent level of reliability.

2.2.1) In the case of using a multi-purpose National Identification Card (Smart Card) as evidence of identification, any one of the following methods may be utilized:

2.2.1.1) Verify the data from a multi-purpose National Identification Card reader against the data on the multi-purpose National Identification Card, or

2.2.1.2) Verify the data on the multi-purpose National Identification Card and verify the status of the card via the electronic verification system of a government agency.

2.2.2) In the case of using a passport as evidence of identification, extract electronic data obtained from the passport, such as data from Near Field Communication (NFC) technology, to verify against the data on the passport; if the data from Near Field Communication technology cannot be verified, other official identification documents issued by the Thai government or state agencies of the country of nationality may be inspected as a substitute.

2.3) Verification of identity in the case where the customer is a legal entity: The Company shall identify and verify the identity of the customer based on complete identification data and obtain other information as prescribed in the Ministerial Regulation on Customer Due Diligence, B.E. 2563 (2020), and may verify the data and evidence against databases of government agencies by implementing the following actions:

2.3.1) Corporate customer registered in Thailand: Verify the Certificate of Incorporation issued by the Registrar not exceeding six months.

2.3.2) In the case of a non-Thai registered legal entity: Verify evidence of legal entity status certified or issued by a reliable agency or organization not exceeding six months.

2.3.3) In the case where the customer is a government agency, government organization, state enterprise, or other state agency that is a legal entity: Verify the letter of intent to conduct transactions, letter of appointment, or power of attorney.

2.3.4) In the case where the customer is a cooperative, foundation, association, club, temple, mosque, shrine, and other legal entities of a similar nature: Verify the letter of intent to conduct transactions, certificate of registration from the relevant authority, letter of appointment, or power of attorney.

3) <u>In the case where the partnership's/company's products or services are low risk:</u>

The Company shall identify and verify the identity of the customer based on complete identification data and proceed to verify the correctness and currency of the identification data and evidence obtained from the customer against reliable data sources, as well as verifying that the customer is the actual owner of such data and evidence,

where customer identity verification for both face-to-face and non-face-to-face interaction shall be implemented as follows:

3.1) In the case of using a multi-purpose National Identification Card or Smart Card as evidence of identification, consideration may be given to utilizing any one of the following methods, or any other method with an equivalent level of reliability:

3.1.1) Verify the data from a multi-purpose National Identification Card reader (Smart Card Reader) via the electronic verification system of a government agency, or

3.1.2) Verify the data from a multi-purpose National Identification Card reader (Smart Card Reader) against the data on the customer's National Identification Card, or

3.1.3) Verify the data against any other database of a government agency, or

3.1.4) Inspect the evidence and certify the correctness of data by personnel to confirm that the customer is the actual owner of such data.

3.2) In the case of using a passport as evidence of identification, consideration may be given to utilizing any one of the following methods, or any other method with an equivalent level of reliability:

3.2.1) Retrieve electronic information obtained from the passport, such as data from Near Field Communication (NFC) technology, to check against the information on the passport, or

3.2.2) Inspect the evidence and certify the correctness of data by personnel to confirm that the customer is the actual owner of such data.

For non-face-to-face customer identity verification, the Company must take and record photographs of the customer to verify and compare the customer's facial image with the customer's image on the multi-purpose National Identification Card, passport, or other reliable data or evidence, in order to prove the actual identity of that customer in lieu of face-to-face interaction.

3.3) Identity verification in the case where the customer is a juristic person: The Company shall identify and verify the customer's identity from complete identification information and obtain other information as prescribed in the Ministerial Regulation on Customer Due Diligence, B.E. 2563 (2020), and may verify the information and evidence against the databases of government agencies by taking the following actions:

3.3.1) In the case of a juristic person registered in Thailand, verify the certificate of incorporation/affidavit issued by the registrar not more than six months prior.

3.3.2) In the case of a juristic person not registered in Thailand, verify the evidence of juristic person status certified or issued by a reliable agency or organization not more than six months prior.

3.3.3) In the case of a customer that is a government sector, government organization, state enterprise, or other government agency that is a juristic person, verify the letter of intent to conduct transactions, letter of appointment, or power of attorney.

3.3.4) In the case of a customer that is a cooperative, foundation, association, club, temple, mosque, shrine, or other juristic persons of a similar nature, verify the letter of intent to conduct transactions, certificate of registration issued by the relevant agency, letter of appointment, or power of attorney.

Nonetheless, once the Company has completed the customer identification process in accordance with the aforementioned criteria, the Company shall conduct a risk assessment for every customer by considering risk assessment factors as prescribed in the Notification of the Anti-Money Laundering Office: Guidelines for Considering Risk Factors on Money Laundering, Terrorism Financing, or the Proliferation of Weapons of Mass Destruction Financing. In the event that the customer's overall risk is found to be at a high-risk level, the Company shall implement enhanced identification procedures by requesting or verifying additional information beyond those prescribed in the Ministerial Regulation on Customer Due Diligence, B.E. 2563 (2020), such as utility bill payment information of the residential address or business premises, copies of business contracts or agreements between the customer and third parties specifically in parts that prove the customer's operations, or verifiable reference data indicating that the customer maintains business relationships with other reliable financial institutions, etc.

Step 4: Customer Due Diligence (CDD)

This is a process to assess and manage risks prior to customer onboarding approval and to monitor the financial movements of the customer's transactions after approving the relationship to detect whether there are any unusual circumstances/transactions that are consistent with their income and occupation, and whether there are reasonable grounds for suspicion. This is to prevent financial institutions and certain types of professions from being used as channels for money laundering/terrorism financing.

In addition, the Customer Due Diligence (CDD) process enhances the quality of Suspicious Transaction Reporting (STR). The reported suspicious transaction information can be utilized as a baseline data for investigating the financial trails of offenders. The objectives of Customer Due Diligence are as follows:

- Whether the customer's information is factual and up to date.
- Whether the customer's transaction pattern is unusual.
- Whether the customer's transaction has other hidden purposes.
- Whether there is an unusually high change in the transaction value.
- Whether the customer's risk level should be adjusted.
- Whether the business relationship with the customer should be continued.

4.1. The Company shall perform Customer Due Diligence under the following circumstances:

- Upon establishing a business relationship with a customer, or
- When there are reasonable grounds for suspicion that it may involve a predicate offense, or
- When there are reasonable grounds for suspicion that it may involve money laundering, or
- When there are reasonable grounds for suspicion that it may involve terrorism financing and the proliferation of weapons of mass destruction financing, or
- When there are doubts regarding the identity information of the customer or the identification of the ultimate beneficial owner.

4.2. The Company shall perform Customer Due Diligence by operating as follows:

4.2.1. <u>In the case of a individual person</u>

1) Identify and verify the customer's identity by using documents, data, or information from reliable sources, which may be obtained in addition to requesting information from the customer. The identification evidence must be strictly the original National Identification Card or original Passport only.
2) Identify the ultimate beneficial owner and implement appropriate measures to verify the identity of the ultimate beneficial owner by using documents, data, or information from reliable sources, which may be obtained in addition to requesting information from the customer. In this regard, evidence of such ultimate beneficial owner identification must be retained, and actions must be taken to obtain sufficient information regarding the ultimate beneficial owner to prove that they are an existing individual person under the law of a specific country and are associated with the customer, primarily considering business relevance. This is except where there is additional information indicating that such person is the ultimate beneficial owner of the customer, despite having no business relevance, such as being related through kinship, politics, or any other contractual arrangements. etc., in order to verify the identification data of the customer's ultimate beneficial owner against the list of designated persons.
3) Sanction screens the data of the customer, the customer's ultimate beneficial owner, and the authorized person (if any) against the list of designated persons in accordance with the law governing the counter-terrorism and proliferation of weapons of mass destruction financing. In this regard, where a power of attorney is granted to establish a business relationship or conduct occasional transactions on behalf of the customer, the Company must verify to ensure that the customer has genuinely authorized the establishment of the business relationship or the occasional transaction on behalf of the customer, and must also perform due diligence on such authorized person, as well as request a power of attorney as evidence of actual authorization.

4) Request information regarding the purpose of the transaction from the customer in order to evaluate its consistency with the intended purpose of such transaction.

5) Continuously monitor the customer's business relationship throughout its duration to ensure it remains consistent with the customer's purpose of establishing the business relationship, the assessed customer risk level, and information regarding the source of income, including other available customer data.

4.2.2. In the case of a juristic person and a legal arrangement

1) Understand the nature of the customer's business, as well as the management or ownership structure, and effective control over such juristic person or legal arrangement. The identification and verification of the identity of such customer shall utilize the following data and evidence:

(1) Name and type, as well as information that can prove the legal status and existence of the juristic person or legal arrangement, such as the organizational structure of the juristic person customer, list of shareholders, Memorandum of Association, etc.

(2) Information regarding the power to control, direct, and bind the juristic person or legal arrangement, including the identification of relevant persons holding senior management positions. In this regard, the Company shall screen such persons against the list of designated persons as well.

(3) Registered address and headquarters address.

2) Identify the ultimate beneficial owner of the customer as follows:

In the case where the customer is a juristic person

(a) Identify the individual person who has ultimate effective control over the juristic person, determined by beneficial interest or ownership, which shall be verified from the list of shareholders of the juristic customer. The Company shall also record the facts regarding the ultimate beneficial owner as evidence.

(b) In the case where there is a doubt regarding the individual person who has ultimate effective control over the juristic person under (a), or if actions under (a) have been taken and no individual person is found to be the ultimate beneficial owner, the Company shall identify the individual person who has ultimate effective control over the juristic person by other means, such as using information from other sources that do not necessarily appear in official government documents or official databases, namely, seeking the customer's ultimate beneficial owner from reliable public media such as newspapers or reliable websites, etc. The Company shall also record the facts of seeking the ultimate beneficial owner as evidence.

(c) If actions under (a) and (b) have been taken and still no individual person is found to be the ultimate beneficial owner, the Company shall implement appropriate measures to verify the individual person who holds the position of senior management of that juristic person. The Company shall record the facts as evidence that it is based on a presumption, due to the inability to locate the ultimate beneficial owner under (a) and (b).

In the case where the customer is a legal arrangement

The Company shall require the trustee or a person holding an equivalent status to a trustee to disclose their status to the Company upon establishing a business relationship or conducting occasional transactions with the customer.

(a) In the case of a trust, identify the names of the settler, trustee, protector, beneficiary or class of beneficiaries, and the individual person who exercises ultimate effective control over the trust, including persons in the chain of control or ownership

(b) In the case of a trust under the law on trusts for transactions in the capital market, identify the names of the settlor, trustee, beneficiary, purpose of the trust, and the assets to be contributed to the trust.

(c) the case of other types of legal arrangements, identify the identity of the person holding an equivalent position to the persons under (a) or (b), as the case may be.

3) Customer Due Diligence must be performed in accordance with item 3.2.1 for the case of a individual person above.

In this regard, for the purpose of Customer Due Diligence, the Company shall monitor and verify the information thoroughly, taking into account the customer's risk level, and conduct Customer Due Diligence. If the Company cannot perform Customer Due Diligence for the customer, it shall refuse the transaction or terminate the relationship with such customer, and shall notify the management in order to report to the Anti-Money Laundering Office (AMLO) pursuant to Section 21/2 of the Anti-Money Laundering Act, B.E. 2542 (1999) and its amendments, and report it as a suspicious transaction.

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Customer Risk Management and Mitigation Policy and Procedures

The Company shall manage and mitigate risks regarding money laundering, terrorism financing, and the proliferation of weapons of mass destruction financing for customers. Employees shall assess risks when transactions are conducted with customers, and operations shall be performed throughout the duration of the business relationship until its termination, as follows:

1. Assess the risk of every customer, including both new and existing customers. In the case of existing customers, this shall be conducted during the periodic review of customer risk data in accordance with the established customer risk levels, taking into account customer-related risk factors as prescribed in the Notification of the Anti-Money Laundering Office: Guidelines for Considering Risk Factors on Money Laundering, Terrorism Financing, or the Proliferation of Weapons of Mass Destruction Financing.
2. Manage risks starting from the assessment process to identify and verify the customer's identity, the determination of risk levels for each individual customer, the monitoring of transaction movements consistent with the customer's risk level, the review of customer verification data consistent with the customer's risk level, and the review of risk assessments until the termination of the business relationship with each customer.
3. If the customer or the customer's ultimate beneficial owner is classified as high risk, Customer Due Diligence shall be performed at the enhanced level, which must be executed in accordance with the following compliance requirements:
    3.1. Seek information from reliable sources or request additional information from the customer regarding the source of funds or assets, and the source of wealth, such as Financial Statements, Salary Certificates, National Identification Card, Employment Contracts, or Tax Returns, etc., as well as the purpose of the transaction, the customer's business operations data, occupation, name and location of the workplace, or the signature of the transacting person.
    3.2. Mandate that senior management shall be the approving authority for establishing a business relationship or conducting transactions with high-risk customers and/or high-risk occasional transaction customers.
    3.3. Upon reviewing customer information and risks, senior management shall evaluate the results of such review to determine whether to approve the continuation of the business relationship with that customer.

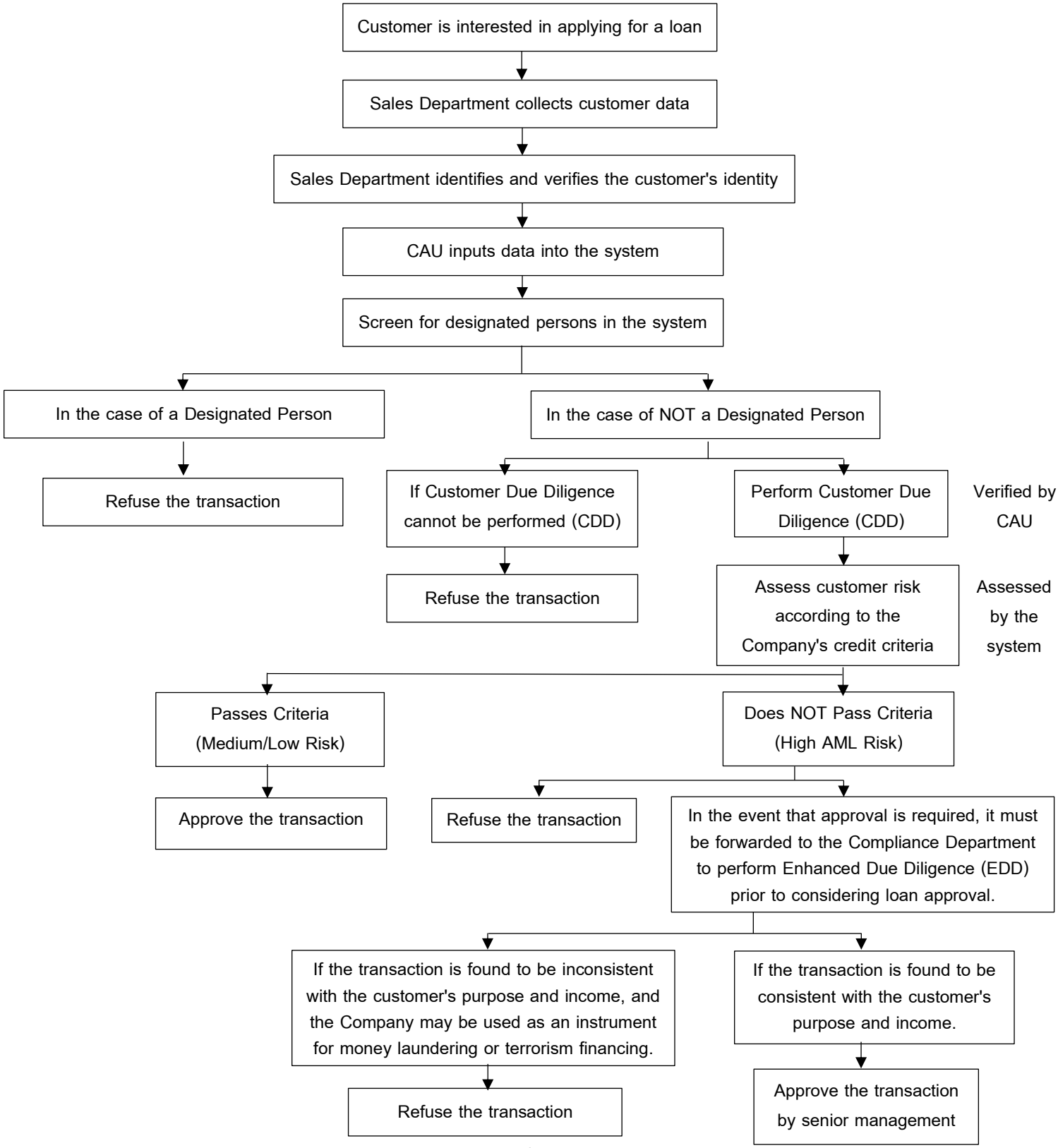
3.4. Establish a financial movement monitoring process for customers and/or occasional transaction customers classified as high risk, by considering increasing the frequency, steps, or nature of business relationship monitoring and transaction movements, as well as increasing the frequency of reviewing customer identification data and the identification of the customer's ultimate beneficial owner.

4. In the event that the customer or the customer's ultimate beneficial owner originates from a high-risk area or country as announced and designated by the Secretary-General, enhanced Customer Due Diligence shall be performed, and countermeasures shall be implemented against the customer by limiting the establishment of business relationships or conducting transactions (limiting the number of times, or limiting the amount of money, or limiting the types of transactions), reviewing the establishment of business relationships, and other measures as announced and prescribed by the Secretary-General.

5. In the event that a customer is at high risk to the extent that it may cause the Company to be used as an instrument for money laundering or terrorism financing, etc., the Company shall refuse the transaction or terminate the relationship with such customer, and report it as a suspicious transaction to the Anti-Money Laundering Office (AMLO).

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

New Customer Onboarding Process



0 2691 5600 | info@srisawadcapital.co.th | www.srisawadcapital.co.th

Policy and Procedures on Risk Assessment of Money Laundering, Terrorism Financing, and Proliferation of Weapons of Mass Destruction Financing for Products or Services

The Company shall manage and mitigate risks regarding money laundering, terrorism financing, and the proliferation of weapons of mass destruction financing for all products, services, and delivery channels of the Company. This applies to cases of launching new products or services, developing new products and business methods, introducing new delivery mechanisms, or utilizing new or developing technologies for both new and pre-existing products, as follows:

Step 1: Collect data on the new product or new service to be offered.

Step 2: Assess product or service risks by considering the following factors:

- Whether it is a product or service that can provide, receive, or convert into cash, where the risk increases according to the amount of cash that such product or service can support.
- Whether it is a product or service that can be transferred or change hands to other persons, where the risk increases according to the value, frequency, speed, or convenience of the transfer or exchange.
- Whether it is a product or service that can be used or applied in foreign countries, where the risk increases if it can be used cross-border.

If any of the following characteristics are met, it shall be considered a product or service with a high risk of money laundering:

1. A product or service that can provide, receive, or convert into cash in high value, or
2. A product or service that can be transferred or change hands to other persons easily, conveniently, and rapidly, or
3. A product or service that can be used or applied in foreign countries, or
4. A product or service characterized by the transfer of monetary value that does not require identification of the transferor or the transferee, or
5. A product or service involving anonymous transactions.

However, if it possesses the following characteristics, it shall be considered a product or service with a low risk of money laundering:

1. A product or service that cannot be exchanged for cash, withdrawn, or refunded in cash within a short period of time, or can be exchanged for cash, withdrawn, or refunded in cash in low value.
2. A product or service that is not a cross-border service and does not generate value in foreign countries or is a cross-border product or service or generates value in foreign countries strictly for the settlement of debts or payment for goods or services of low value.
3. A product or service that cannot store monetary value in a large amount and cannot transfer value to others or can transfer only in a low value.

The total transaction value under 1), 2), and 3) combined must not exceed 50,000 Baht per month.

Step 3: Define appropriate risk mitigation measures for products or services in accordance with the law, in order to prevent products or services from being used as instruments for money laundering and terrorism financing.

Step 4: Review product or service risks, delivery channels, and review risk mitigation measures to ensure appropriateness and effectiveness.

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Employee Training Policy and Procedures

To ensure that employees possess knowledge and understanding of anti-money laundering, counter-terrorism and proliferation of weapons of mass destruction financing, and can correctly perform their duties as prescribed by law, the Company has established guidelines for personnel training and development as follows:

1. **Employee Screening**

Prior to hiring or assigning duties related to anti-money laundering, counter-terrorism and proliferation of weapons of mass destruction financing, it is required to screen the employees' names against the list of designated persons or conduct a criminal record check.

2. **Employee Training**

Training Plan for New Employees

The Company shall provide training for new employees to reinforce sufficient knowledge and understanding regarding the laws, rules, policies, and operational guidelines related to compliance with the anti-money laundering law, and the law on counter-terrorism and proliferation of weapons of mass destruction financing. This is to enable employees to perform duties in preparing or controlling the screening of designated persons, Customer Identification (KYC), identification and Customer Due Diligence (CDD), institutional risk assessment, customer risk assessment and management, product/service/delivery channel risk assessment, transaction reporting, internal audit, training attendance, data retention, and policy updates, within 30 days from their commencement date.

Training Plan for Existing Employees

The Company shall promote and provide management and employees with enhanced knowledge and understanding in operating under policies and guidelines related to compliance with the anti-money laundering law, and the law on counter-terrorism and proliferation of weapons of mass destruction financing appropriate for all levels of employees on a continuous basis. This is to ensure operations comply with the law at least once every 1 year. In the event that the laws or policies concerning anti-money laundering, counter-terrorism, and the proliferation of weapons of mass destruction financing are amended, additional training shall be provided, with the participating employees as follows:

1. Executive-level management employees responsible for supervising compliance with the law governing anti-money laundering, and the law on counter-terrorism and proliferation of weapons of mass destruction financing.
2. Operational-level employees responsible for monitoring compliance with the anti-money laundering law, and the law on counter-terrorism and proliferation of weapons of mass destruction financing (Compliance).
3. Employees operating in internal audit regarding anti-money laundering, and counter-terrorism and proliferation of weapons of mass destruction financing (Audit).
4. Employees involved in operations related to preparing or controlling the preparation of transaction reports, Customer Identification (KYC), and Customer Due Diligence (CDD), such as customer onboarding staff,

staff performing identification and Customer Due Diligence, staff conducting institutional risk assessment, staff conducting customer risk assessment and management, staff conducting product/service/delivery channel risk assessment, staff reporting transactions, and data retention staff, etc.

In this regard, the Company shall retain copies of employee training evidence, including copies of evidence showing that such employees have completed the training, within the business premises under secure methods, and shall be capable of retrieving or submitting the details as requested by the Anti-Money Laundering Office (AMLO).

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Transaction Reporting Policy and Procedures

The Company requires transaction reporting to the Anti-Money Laundering Office (AMLO) as follows:

"**Cash Transaction**" means only cash-receiving activities between the customer and the Company, excluding wire transfers into the bank account of either party, and must have a value of 500,000 Baht or more.

"**Suspicious Transaction**" means a transaction where there is a reasonable ground to believe that it is conducted in order to avoid the application of the Anti-Money Laundering Act, B.E. 2542 (1999), or a transaction that may be connected with the commission of a predicate offense or terrorism financing, regardless of whether it is a single transaction or multiple transactions, and shall also include an attempted transaction.

1. **Criteria for Transaction Reporting** (Timeline, Form, Method of Submission)

Transaction Subject to Reporting	Reporting Form	Submission Timeline for Transaction Report	Method of Form Submission
Cash Transactions • Value of 500,000 Baht or more	AMLO Form 1-05-6	Report within the following month from the month in which the transaction is conducted (should not exceed the last day of the following month).	Submit to the officer at the AMLO office, or send via registered mail with acknowledgment of receipt, or submit as electronic data in accordance with the law on electronic transactions through the ERS system.
Suspicious Transactions	AMLO Form 1-05-10	Report within 7 days from the date the reasonable ground for suspicion is discovered, or report without delay for suspicious transactions discovered subsequently.	

2. **Transaction Reporting Procedures**

The Company has a duty to monitor all transactions of each individual customer by establishing a screening and verification process for transaction reports prior to submission to the Anti-Money Laundering Office (AMLO). This is to ensure that reporting is accurate and complete in accordance with the criteria prescribed by law.

In this regard, if a reportable suspicious transaction is identified, the verification procedures are defined as follows:

Step 1: Conduct verification against customer data, such as the consistency of the transaction value with the customer's income or economic standing, coupled with the consistency with the economic conditions of investment at that time, as well as other factors that may be considered under organizational policies and guidelines.

Step 2: Review the customer's past transaction behavior to determine the frequency of similar transactions in the past, or if there are any additional reasonable grounds for suspicion.

Step 3: Summarize the results of the transaction analysis and report the verification findings to the authorized management responsible for reviewing suspicious transactions.

Step 4: In the event that reporting to AMLO is deemed appropriate, the said authorized management shall sign for approval to submit the customer's transaction report as a suspicious transaction (in the case where reporting is deemed inappropriate, such record shall be retained as evidence).

The Company considers suspicious transactions under 2 separate scenarios as follows:

(1) When the Company detects a suspicious transaction on its own, such as:

- The transacting person is required to conduct a cash transaction with a value of 500,000 Baht, but intends to avoid being subject to transaction reporting by structuring the transaction thresholds unusually from general transacting persons.
- The transacting person is associated with money laundering or terrorism financing, etc.
- The transacting person is capable of fully settling debts prior to the contractual maturity date within a short timeframe, even though at the time of entering into the contract, the customer demonstrated a level of financial status that unlikely possessed the capability to close the contract so rapidly (rendering the transaction inconsistent with their financial status).
- The customer fails to provide personal data or fails to provide identification evidence such as a National Identification Card/Passport.

The Company shall report suspicious transactions by submitting the reporting form to AMLO within seven days from the date the reasonable grounds for suspicion exist.

(2) When the Company receives a written notification of an asset seizure or freezing order from a government agency with competent authority in prosecuting offenses related to predicate offenses, which is divided into 2 scenarios as follows:

- In the case of receiving a notification of an asset seizure or freezing order from the Anti-Money Laundering Office (AMLO), the Royal Thai Police, or a police station, the Company may exercise its discretion to

perform a retrospective transaction review of the customer subject to such seizure or freezing order, counting backward from the date the said order was received, by utilizing the Customer Due Diligence (CDD) process. This is to identify any reasonable grounds for suspicion in the customer's transactions, including those of the customer's ultimate beneficial owner (UBO) or associated persons, that occurred prior to receiving the asset seizure or freezing order from AMLO. If any prior or related transactions are found to have reasonable grounds for suspicion, the Company shall consider reporting them as a suspicious transaction by submitting the reporting form to AMLO within seven days from the date the reasonable grounds for suspicion exist.

- In the case of receiving a notification of an asset seizure or freezing order from other government agencies with competent authority in prosecuting cases related to predicate offenses, such as the National Anti-Corruption Commission (NACC), the Public Sector Anti-Corruption Commission (PACC), or the Office of the Narcotics Control Board (ONCB), the Company shall report it as a suspicious transaction by submitting the reporting form to AMLO within seven days from the date the reasonable grounds for suspicion exist (the date on which the Company receives the written notification of the asset seizure or freezing order from that respective agency).

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Policy and Procedures on Data and Document Retention

The Company requires the retention of data and documents in order to comply with Section 22 and Section 22/1 of the Anti-Money Laundering Act, B.E. 2542 (1999) as follows:

1. **Identification documents** must be retained for a period of 5 years from the date of account closure or termination of relationship with the customer, or the date of conducting a transaction with an occasional customer whose transaction reaches the threshold requiring identification.
2. **Transaction documents and factual records** must be retained for a period of 5 years from the date such transaction was conducted or such factual record was made.
3. **Customer Due Diligence documents** must be retained for a period of 10 years from the date of account closure or termination of relationship with the customer, or the date of conducting a transaction with an occasional customer whose transaction falls under the criteria requiring Customer Due Diligence.

Nonetheless, the Company may consider retaining all documents for a period of 10 years for consistency, unless otherwise notified in writing by the Secretary-General of AMLO.

In this regard, the Company retains the data and document details in accordance with the aforementioned anti-money laundering law by storing them as (documents or electronic data). The criteria for retaining such data and documents are as follows:

1. Capable of being stored, accessed, or retrieved without any alterations to the data.
2. Capable of retaining details in a format that can accurately display and manifest the received information.
3. Capable of transferring data details into recording media or transmitting them through other information systems as prescribed by the Anti-Money Laundering Office (AMLO).
4. Capable of being retained accurately and completely under secure and reliable methods, and capable of being retrieved or submitted as prescribed by the Office.

Note * Information relating to Customer Due Diligence includes:

1. Customer transaction data.
2. Transaction verification data conducted by the customer for risk management regarding transactions suspected of being potentially involved in money laundering or terrorism financing.
3. Update data of various customer information used for identification, verification, and data taken into consideration for risk management.
4. Customer risk rating data.
5. Information on the implementation of Customer Due Diligence (CDD), which includes: (a) Identification and verification of the identity of the customer, legal arrangement, and ultimate beneficial owner (UBO); (b) Screening of the data of the customer, legal arrangement, and the customer's ultimate beneficial owner against the list of designated persons under the law governing the counter-terrorism financing; (c) Intended purpose of establishing the business relationship; (d) Results of financial movement monitoring or transaction movement monitoring throughout the duration of the relationship with the customer.

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Internal Control Policy and Procedures on Anti-Money Laundering and Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing (AML/CFT)

The Company defines the methods for internal control as follows:

1. Mandate that employees operating in compliance functions (Compliance) shall be responsible for acknowledging reports on operational compliance monitoring results to ensure alignment with the law governing anti-money laundering and the law on counter-terrorism and proliferation of weapons of mass destruction financing, in order to utilize the findings obtained from internal audits of anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing operations within the Company to expedite corrective actions and improvements to operations in accordance with the law, and to further develop and update policies.
2. Mandate that the selection of companies/third parties/employees to perform internal audit functions shall be limited to those who have completed training on anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing with the Anti-Money Laundering Office (AMLO) or completed training from private entities certified by AMLO to conduct training on its behalf, prior to employment for operations regarding anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing.
3. Establish an internal audit plan for anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing by defining scopes to comprehensively cover all aspects as required by law.
4. Mandate training for employees operating in anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing to possess knowledge and understanding regarding anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing from prior to commencing work and on a continuous basis.
5. Mandate that supervisors of compliance function employees shall perform internal audit duties, mandating internal audits regarding operating systems and compliance with the laws governing anti-money laundering, terrorism financing, and the proliferation of weapons of mass destruction financing, which possesses independence and is not operational personnel in anti-money laundering and counter-terrorism and proliferation of weapons of mass destruction financing.

บริษัท ศรีสวัสดิ์ แคปปิตอล 1969 จำกัด (มหาชน)
99/392 อาคารศรีสวัสดิ์ ชั้น 1,5,6
ซอยแจ้งวัฒนะ 10 แยก 3 (เบญจมิตร)
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่
กรุงเทพมหานคร 10210
เลขประจำตัวผู้เสียภาษี 0107536000722

Policy and Guidelines on Compliance with the Law Governing Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing

The Company defines the guidelines regarding the prevention of terrorism financing and the proliferation of weapons of mass destruction financing as follows:

1. **Measures on Customer Sanction Screening and Refusal of Transactions**

The Company shall screen the names of all customers, ultimate beneficial owners (UBOs), and authorized persons (if any) against the list of designated persons in accordance with the law governing the counter-terrorism and proliferation of weapons of mass destruction financing prior to every transaction. If the screening does not match a designated person, employees may proceed with the transaction. However, if the screening and data verification confirm that the said customer is indeed a designated person, the transaction shall be refused. In the case of an existing customer, if found to be a designated person, the Company shall report the designated person's customer data to the Anti-Money Laundering Office (AMLO) within 10 working days from the date of discovery using Form PKR. 04, and report it as a suspicious transaction using AMLO Form 1-05-10 within 7 days from the date of discovery.

2. **Measures on Maintaining Up-to-Date Designated Person Lists**

The Company shall continuously update the designated person database by screening names prior to boarding every customer and at appropriate regular intervals. If it is found that AMLO has announced or delisted any designated persons, the Company shall update its designated person database in accordance with the latest list announced by AMLO.

3. **In the Case of High-Risk Areas or Countries Regarding Terrorism and Proliferation of Weapons of Mass Destruction Financing**

The Company shall perform Customer Due Diligence at the highest enhanced level in the event that a customer holds nationality, domicile, or current address in areas or countries with high risks regarding terrorism and the proliferation of weapons of mass destruction financing.

4. **Post-Discovery Procedures upon Identifying a Designated Person**

Scenario 1: Where the screening identifies the customer as a designated person but the Company does not possess any assets belonging to the said designated person, the Company shall proceed to report the information of the customer or former customer who is a designated person to AMLO. within 10 working days from the date of discovery of that customer's status as a designated person using Form PKR. 04, and report the suspicious transaction using AMLO Form 1-05-10 within 7 days from the date of discovery.

Scenario 2: Where the screening identifies the customer as a designated person and the Company possesses the assets of that designated person (receiving funds from the designated person prior to performing the sanction screening), the following actions shall be taken:

(1) Freeze assets within 24 hours from the time of knowing that the person is a designated person.

(2) Report information regarding the frozen assets. Upon freezing the assets of the designated person, the Company shall report the information of the frozen funds or assets to the Anti-Money Laundering Office (AMLO) using Form PKR. 03 within 10 working days from the date the assets of the designated person were frozen.

(3) Report customer information. Report the designated person's customer data to AMLO within 10 working days from the date of discovery of that customer's status as a designated person using Form PKR. 04.

(4) Report the suspicious transaction to AMLO (AMLO Form 1-05-10) within 7 days from the date of discovery.

5. Product or Service Risk Assessment

To ensure that existing products or services, as well as those to be newly created or developed, or provided in the future, will not be used as channels for terrorism financing and the proliferation of weapons of mass destruction financing, a product or service risk assessment is mandated, along with the definition of risk mitigation measures. Furthermore, strict screening of every customer prior to any transaction is required to prevent being used as a channel for terrorism financing and the proliferation of weapons of mass destruction financing.

In this regard, a plan for updating policies and procedures to comply with the law has been established, which shall be reviewed and updated at least once a year or when there are changes in the law.

This policy shall be effective from 1 December 2022.