The Compilation of Directives
For Reporting Entities
to Implement the Law on Anti-Money Laundering
and Combating the Financing of Terrorism

Cambodia Financial Intelligence Unit

2023

The Compilation of Directives For Reporting Entities to Implement the Law on Anti-Money Laundering and Combating the Financing of Terrorism

CONTENT

1. Directive on Remittance and Wire Transfer 1
2. Directive on Correspondent Banking and Other Similar Relationship.....6
3. Directive on Internal Controls for Reporting Entity 9
4. Directive on Customer Due Diligence Measures 16
5. Directive on the Designated Threshold for Customer Due Diligence for Casinos and Other Gambling Institutions.....26
6. Directive on Risk Based Supervision 27

Directive
on
Remittance and Wire Transfer

KINGDOM OF CAMBODIA

NATION RELIGION KING

Cambodia Financial Intelligence Unit

N° ...B12 022 010 S.K.N.N...

Unofficial Translation

Directive
On
Remittance and Wire Transfer

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0620/021 dated 27 June 2020 the Cambodia Financial Intelligence Unit (CAFIU) issues Directive on Remittance and Wire Transfer. This Directive shall be also applicable to, where relevant, their agents.

1. Scope

This Directive shall apply to reporting entity referred to in Article 4 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) when it participates in remittance and wire transfer transaction.

2. Definition

Wire Transfer shall mean any transaction carried out on behalf of an originator between financial institutions by electronic means with a view to making an amount of funds available to a beneficiary person at a beneficiary financial institution, irrespective of whether the originator and the beneficiary are the same person.

Originator shall mean the account holder who allows the wire transfer from that account, or where there is no account, the natural or legal person that places the order with the ordering financial institution to perform the wire transfer.

Beneficiary shall mean the natural or legal person or legal arrangement who is identified by the originator as the receiver of the requested wire transfer.

Cross-border Wire Transfer shall mean any wire transfer where the ordering financial institution and beneficiary financial institution are located in different countries.

Domestic Wire Transfer shall mean any wire transfer where the ordering financial institution and beneficial institution are located in the same country.

Money or Value Transfer Service shall mean financial service of receiving cash, check, other monetary instruments or other stores of value instruments, and the payment of a corresponding sum in cash to beneficiary by means of a communication, message, transfer or through a clearing network to which the MVTS provider belongs.

P.O. Box 67 #22-24 Preah Norodom Blvd, Phnom Penh, Cambodia www.nbc.org.kh/cafiu cafiu_info@nbc.org.kh

Agent shall mean natural or legal person who provides money or value transfer service on behalf of money or value transfer service provider.

3. Wire Transfers – Origination

3.1. The reporting entity conducting or participating in cross-border wire transfer transactions with an amount equal to or above 4,000,000 (four million) Riels or foreign currency equivalent shall include and verify the originator information in any cross-border wire transfers as following:

a) the full name of the originator;

b) the originator account number, or where no account number is available, a unique transaction reference that will permit the transaction to be traced;

c) the originator's address or customer identification number or national identity number or personal identification number issued by competent authorities or date and place of birth; and

d) the originator's purpose.

3.2. The reporting entity conducting or participating in cross-border wire transfer transactions with an amount equal to or above 4,000,000 (four million) Riels or foreign currency equivalent shall include and verify the beneficiary information in any cross-border wire transfers as following:

a) the full name of the beneficiary;

b) the beneficiary account number where such an account is used to process the transaction, or where no account number is available, a unique transaction reference that will permit the transaction to be traced.

3.3. Where several cross-border wire transfers from a single originator the total value of which is equal to or above 4,000,000 (four million) Riels or foreign currency equivalent within one day, reporting entity shall bundle those transfers in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information in accordance with Point 3.1 and full beneficiary information in accordance with Point 3.2 of this Directive and shall be accurately verified that is traceable within the beneficiary country.

3.4. Cross-border wire transfer for less than 4,000,000 (four million) Riels or foreign currency equivalent shall be accompanied by the information referred to in Point 3.1 (a), (b) and (d) and Point 3.2 (a) and (b) of this Directive.

3.5. The information accompanying cross cross-border wire transfers referred to in Point 3.4 of this Directive need not be verified unless a suspicion of ML/TF arises or the transaction may involve with a predicate offence or ML/TF, in which case verification of the customer's details shall be completed as soon as practicable.

3.6. For domestic wire transfer conducted between domestic financial institutions, the originator information referred to in Point 3.1 and beneficiary information referred to in Point 3.2 of this Directive shall accompany the transfer, unless the information can be made available to the beneficiary financial institution by other means. Where the information was made available by other means, reporting entity shall only include the account number or unique transaction reference of originator and beneficiary with the transfer instruction to the beneficiary reporting entity.

3.7. Where full originator information has not been included in a domestic wire transfer, this information shall be made available by the ordering reporting entity within three business days of receiving the request either from the beneficiary financial institution or from CAFIU.

3.8. The reporting entity shall maintain all originator and beneficiary information in accordance with Article 11 of the Law on AML/CFT.

3.9. The reporting entity shall not execute the wire transfer, if the originator of a wire transfer, that is not able to comply with the requirements of Point 3.1 of this Directive.

4. Wire Transfers – Intermediation

4.1. Where a reporting entity is an intermediary in processing a wire transfer prepared by another financial institution acting for an originator it must ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.

4.2. Where technical limitations prevent the required originator and beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a reporting entity acting as an intermediary shall keep records of all information received from the ordering financial institution or another intermediary financial institution for at least five years from the date of the transaction.

4.3. The reporting entity that is acting as an intermediary in processing wire transfer shall have procedures in place, that are consistent with straight-through processing, that enable it to identify incoming cross-border wire transfers that lack the originator and beneficiary information referred to in Point 3.1 and 3.2 of this Directive.

4.4. The reporting entity that acts as an intermediary in processing wire transfer shall have risk-based policies and procedures in place for determining:

a) When to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and

b) the appropriate follow-up actions which may include restricting or terminating business relationships.

5. Wire Transfer – Beneficiary Transaction

5.1. The reporting entity providing services for customers who are the beneficiary of incoming wire transfers shall have procedures in place for undertaking post-event monitoring or real-time monitoring of incoming wire transfers that identifies cross-border wire transfers that have insufficient and incorrect information of the originator or beneficiary referred to in Point 3.1 and 3.2 of this Directive.

5.2. The reporting entity processing an incoming wire transfer equal to or above 4,000,000 (four million) Riels or foreign currency equivalent shall verify the identity of the beneficiary if not previously identified and verified in accordance with the requirements of the Law on AML/CFT or Point 3.1 and 3.2 of this Directive. Any information derived from the identification or verification of the beneficiary shall be retained in accordance with Article 11 of the Law on AML/CFT.

5.3. The reporting entity that acts for beneficiaries of incoming wire transfers shall have risk-based policies and procedures in place for determining:

a) when to execute, reject or suspend a wire transfer lacking required originator or beneficiary information; and

b) the appropriate follow-up actions which may include restricting or terminating business relationships.

6. Money or Value Transfer Service

6.1 The reporting entity offering Money or Value Transfer Service whether directly or as an agent shall comply with all relevant requirements in this Directive although they operate, directly or through their agents, in any country.

6.2 The reporting entity offering Money or Value Transfer Service controlled both the ordering and the beneficiary sides of a transaction shall:

a) take into account all information from both the ordering and beneficiary sides in order to determine whether a STR has to be submitted to the CAFIU;

b) file a STR in any country affected by the suspicious remittances or Money or Value Transfer Service and make relevant transaction information available to the CAFIU; and

c) monitor the agent's activity on the implication of AML/CFT.

7. Targeted Financial Sanctions

The reporting entity shall, in process of wire transfers, take freezing action and comply with prohibitions on conducting transactions with designated natural and legal persons, as per obligations set out in the Sub-decree on Freezing of Property of Designated Terrorists and Organizations relating to the prevention and suppression of terrorist activities and the financing of terrorism, inclusive of United Nations Security Council Resolutions 1267 and 1373 and any successor resolutions.

8. Sanction

Any reporting entity which do not comply with this Directive shall be penalized as stated in Article 36 and Article 37 of the AML/CFT Law.

Up on receiving this directive, all reporting entities shall effectively implement this Directive from the date of the signature.

Phnom Penh, 11 January 2022
Cambodia Financial Intelligence Unit
Head
(Signed and Sealed)

SAY SAM ATH

Attention to:
- Office of the Council of Ministers
- National Coordination Committee on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Proliferation
- Cambodia Financial Intelligence Unit's Board of Directors
- Documentations-Archives

Directive
on
Correspondent Banking and Other Similar Relationship

KINGDOM OF CAMBODIA

NATION RELIGION KING

Cambodia Financial Intelligence Unit

Nº ...B12 022 009 SKNN...

Unofficial Translation

Directive

On

Correspondent Banking and Other Similar Relationship

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0620/021 dated 27 June 2020 the Cambodia Financial Intelligence Unit (CAFIU) issues Directive on Correspondent Banking and Other Similar Relationship.

1. Scope

This Directive shall apply to reporting entity referred to in Article 4 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) when it involves in correspondent banking or other similar relationship.

2. Definition

Correspondent Banking shall mean the provision of banking services by one institution called correspondent institution to another institution called respondent institution.

Similar Relationship shall mean the relationship undertaken for securities transactions or funds transfers, for the financial institution that is operating outside Cambodia, whether as principal or for its customers.

Shell Bank and Financial Institution shall mean a bank or financial institution officially recognized, incorporated, formed, established, registered or licensed in a country or jurisdiction where the bank or financial institution has no physical presence and which is unaffiliated with a financial group that is subject to effective consolidated supervision.

Payable through Account shall mean a correspondent account that is used directly by third parties to transact business on their own behalf.

3. Correspondent Banking

3.1. The reporting entities shall take the necessary measures to ensure that they are not exposed to the threat of Money Laundering or Terrorist Financing (ML/TF) through correspondent accounts they have with other domestic financial institutions or foreign financial institutions. The reporting entity shall establish policies and procedures for correspondent banking and other similar relationship including risk management and mitigation measures.

P.O. Box 67 #22-24 Preah Norodom Blvd, Phnom Penh, Cambodia www.nbc.org.kh/cafiu cafiu_info@nbc.org.kh

3.2. The reporting entity entering a correspondent relationship shall gather and assess at least the following information on the respondent institutions:

a) board of director and management;

b) full understanding of nature and purposes of business activities and products or services;

c) countries or jurisdictions in which it operates;

d) its reputation determined from publicly or any available sources of information;

e) subjected legislation, regulation, and supervision including whether it has been subject to money laundering or terrorist financing investigation or regulatory or supervisory actions;

f) AML/CFT measures and controls; and

g) annual reports.

3.3. A reporting entity shall establish or continue a correspondent banking relationship only if senior management approves the relationship upon being satisfied:

a) that the assessment of the information gathered demonstrates that the risk of ML/TF that can be associated with the relationship is low and can be managed or mitigated; and

b) the AML/CFT responsibilities of both parties to the relationship are clearly understood and documented.

3.4. The reporting entity shall terminate, or not establish or continue the correspondent relationships or occasional transactions with shell banks and financial institutions.

3.5. The reporting entity shall satisfy itself that the respondent financial institutions do not permit their accounts to be used by shell banks and financial institution.

3.6. The reporting entity shall exercise Enhanced Customer Due Diligence (EDD) referred to in Point 4.7 of Directive on Customer Due Diligence Measures with respect to correspondent or respondent institutions which allow direct use of the correspondent account by their customers. The reporting entity shall implement Customer Due Diligence (CDD) referred to in Point 4.5 of Directive on Customer Due Diligence Measures for such customers as required for intermediaries introducing business. In addition, the reporting entity shall ensure that:

a) the respondent financial institutions have conducted CDD and ongoing monitoring of its business for customers having direct access to the payable-through account and

b) the respondent institutions can make available CDD information upon request by reporting entity or by CAFIU;

3.7. The reporting entity shall pay special attention to new and existing correspondent banking and other similar relationship with financial institutions from countries or jurisdictions which have insufficiently implemented internationally accepted AML/CFT measures or which are under ML/TF investigations and not subject to appropriate AML/CFT regulation and supervision. EDD shall be applied in relation to transactions conducted through such correspondent banking and other similar relationship.

3.8. Reporting entity shall review existing correspondent banking and other similar relationship to meet requirements stated in this Directive.

4. Sanction

Any reporting entity which do not comply with this Directive shall be penalized as stated in Article 36 and Article 37 of the AML/CFT Law.

Up on receiving this directive, all reporting entities shall effectively implement this Directive from the date of the signature.

Phnom Penh, 11 January 2022

Cambodia Financial Intelligence Unit
Head
(Signed and Sealed)

SAY SAM ATH

Attention to:
- Office of the Council of Ministers
- National Coordination Committee on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Proliferation
- Cambodia Financial Intelligence Unit's Board of Directors
- Documentations-Archives

Directive
on
Internal Controls for Reporting Entity

KINGDOM OF CAMBODIA

NATION RELIGION KING

Cambodia Financial Intelligence Unit

Nº ...B12 022 008 S.K.N.N

Unofficial Translation

Directive

On

Internal Controls for Reporting Entity

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0620/021 dated 27 June 2020 the Cambodia Financial Intelligence Unit (CAFIU) issues Directive on Internal Controls for Reporting Entity.

1. Scope

This Directive shall apply to reporting entity referred to in Article 4 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT). This Directive should also applicable to reporting entity that are part of a financial group or reporting entity that have foreign branches or majority owned subsidiaries.

2. Risks and Internal Controls

2.1. The reporting entity shall be aware of and understand the ML/TF risks that are required to be assessed in accordance with Article 8 of the Law on AML/CFT and relevant regulations. The reporting entity shall ensure that the result of risk assessment is disseminated, for information and training purposes, to all staffs and senior managements.

2.2. The reporting entity shall ensure that internal policies, procedures and system and controls for AML/CFT are in place and effectively implemented. The internal policies, procedures and system and controls shall detail customer due diligence (CDD) procedures, risk management practices, record keeping requirements, on-going CDD requirements, procedures for reporting transactions and other relevant requirements as required by the Law on AML/CFT in compliance with legal requirements and commensurate with the nature and size of the reporting entity, complexity of operations and the assessed levels of ML/TF risk.

2.3. The reporting entity shall oversee and review internal policies, procedures and system and controls of the overall AML/CFT policies, procedures and controls.

2.4. The reporting entity shall review and assess regularly and keep up to date the internal policies, procedures and system and controls in line with the changes and developments in its products, services, delivery channels and technology systems, as well as trends in ML and TF techniques at both sectoral and national levels. The reporting entity shall implement the necessary changes to the internal policies, procedures and system and controls to ensure that they are sound and appropriate and commensurate with currently assessed risk at institutional, sectoral and national levels.

P.O. Box 67 #22-24 Preah Norodom Blvd, Phnom Penh, Cambodia www.nbc.org.kh/cafiu cafiu_info@nbc.org.kh

2.5. The reporting entity shall ensure that an independent internal and external audit is regularly undertaken that reviews the adequacy of the internal policies, procedures and system and controls having regard to the requirements of laws and regulations related to AML/CFT and the effectiveness of their implementation.

2.6. The reporting entity shall ensure that the roles and responsibilities of the independent internal auditor are clearly defined and documented and at least include:

a) testing the effectiveness of the internal policies, procedures and system and controls;

b) reporting on the adequacy of AML/CFT control mechanisms including the appointment of compliance officer, training and awareness programs for staff, where relevant, its agents and distributors, employee screening mechanisms and AML/CFT internal audit manual; and

c) reporting on whether measures put in place are in line with current developments and changes of the relevant AML/CFT requirements.

2.7. The reporting entity shall ensure that audit findings are reported on a regular basis. The audit report shall highlight inadequacies of any AML/CFT measures and control systems within the reporting entity. The reporting entity shall ensure that necessary steps are taken to rectify the situation.

2.8. The reporting entity shall put in place an adequate management information system for identifying, detecting and scrutinizing business relationships and occasional transactions, that they suspect or have reasonable grounds to suspect that such relationship is related to proceeds from an unlawful activity or the customer involving ML or TF. The management information system shall provide reporting entity timely information on a regular basis to enable them to detect and report suspicious activities.

2.9. Reporting entity shall ensure that the reporting system put in place for the detection and submission of suspicious transaction reports and/or relevant documents to CAFIU is operated in a secured and confidential manner.

3. Employee Integrity

Reporting entity shall ensure that an employee assessment system is established to adequately screen and assess its employees, both existing and new, to ensure that the competency and the integrity of its employees are not compromised. The employee assessment system shall at least examine and record personal information including criminal records, employment and financial history as well as regulatory and supervisory actions against, of its employees as part of the recruitment process and existing employees.

4. Anti-Money Laundering and Combating the Financing of Terrorism Compliance Officer

4.1. Reporting entity shall appoint a compliance officer and attach his/her curriculum vitae pursuant to Article 17 of Law on AML/CFT. The appointed compliance officer shall be subject to an approval from CAFIU.

4.2. Reporting entity shall inform the CAFIU upon the change in the appointment or resignation of the compliance officer and designate a senior officer to be temporary contact point with CAFIU in order to ensure continuity of the AML/CFT obligations. The reporting entity shall submit the appointment of new compliance officer for approval from CAFIU within 1 (one) month after the change in the appointment or resignation of the compliance officer.

4.3. Reporting entity shall ensure that the roles and responsibilities of the compliance officer are clearly defined and documented. The roles and responsibilities of the AML/CFT compliance officer should include at least ensuring:

a) implementation of the AML/CFT policies;

b) the establishment, development and effective implementation of appropriate AML/CFT procedures including customer acceptance policy, CDD, risk management practice, record keeping, on-going monitoring, reporting of transactions and other relevant requirements of the Law on AML/CFT;

c) regular monitoring and assessment of AML/CFT methods to ensure that AML/CFT internal policies, procedures and system and controls are sufficient to address the changing methods and trends of predicate offence and money laundering and financing of terrorism;

d) the channel of communication between the compliance officer and employees and/or other relevant employees is secured and that any information is kept confidential;

e) all employees are aware of AML/CFT measures including policies, procedures, control mechanisms and channels of reporting to ensure the effectiveness of such measures;

f) the identification of money laundering and financing of terrorism risks associated with new products or services, delivery channel or arising from the reporting entity's operational changes, such as the introduction of new technology and processes.

g) submission of transaction reports as set in Article 12 of the Law on AML/CFT to CAFIU;

h) management of the ongoing ML/TF risk assessment process; and

i) employee performance of pursuant to the requirements of policy, procedure, law and regulation related to AML/CFT and CAFIU recommendations.

4.4. Compliance officer shall have necessary knowledge, expertise and experiences to responsibly and effectively discharge his/her roles and responsibilities that shall not be interfered by any person. The compliance officer should have access and rights to have all documents and information from units, subsidiaries, and branches related to customer account and transactions.

4.5. The AML/CFT policies and procedures of reporting entity shall permit the compliance officer to directly obtain reports of unusual activities from relevant employees even if he/she

does not know precisely what the underlying unlawful activity is or whether such activities have occurred. Once this report is satisfied with the requirement in Article 12 and Article 13 of the Law on AML/CFT, the compliance officer shall submit the suspicious transaction report to CAFIU.

5. Staff Training and Awareness Programs

5.1. Reporting entity shall have an adequate ongoing awareness and training programs on AML/CFT for its employees, where relevant, its agents and distributors, that are commensurate with the size of the reporting entity's business and its level of ML and TF risk. The training and awareness programs must be extended to all new and existing employees.

5.2. The AML/CFT training programs shall ensure the effective implementation of AML/CFT policies and procedures and the understanding of ML/TF risks associated with the reporting entity.

5.3. Reporting entity shall ensure that proper channels of communication are in place to inform all levels of employees in reporting entity, agents and distributors of the applicable AML/CFT policies and procedures.

5.4. Reporting entity shall ensure that employees are aware of AML/CFT policies, internal controls and manual in place and the requirements as specified in laws and regulations related to AML/CFT.

5.5. The reporting entity shall develop and update internal AML/CFT manual which at least contains:

a) the laws and regulations related to AML/CFT;

b) the FATF Recommendations and Interpretive Notes; and

c) Other guidelines or procedures issued by CAFIU

5.6. The reporting entity shall adapt at least the following training packages for the various sectors of employees within their institutions:

a) New Employees

A general background to laws and regulations on AML/CFT and ML/TF theories.

b) Front-Line Employees

Employees who deal directly with the customers shall be trained at least in identifying transactions, the measures to be taken once a transaction is deemed to be suspicious, factors that may give rise to suspicions, large volume transaction reporting and enhanced customer due diligence.

c) Employees - Account Opening/New Customers

Employees, who are responsible for account opening or the acceptance of new customers, shall receive the equivalent training given to front-line employees and shall at least be trained in customer identification and verification, opening of accounts and establishing business relationship with customers.

d) Supervisors and Managers

Supervisors and managers shall receive a higher level of instruction covering all aspects of AML/CFT including law, regulations, policies, and procedures of which include the penalties for non-compliance to the AML/CFT requirements.

5.7. These training and awareness programs shall be regularly conducted and kept up to date with refresher courses provided for employees. New employees shall be trained within 3 (three) months after the commencement of employment and front-line employees, supervisors and managers shall have at least refresher training annually.

6. Targeted Financial Sanctions Against the Financing of Terrorism

6.1 Reporting entity shall take the necessary measures to ensure compliance with the United Nations Security Council (UNSC) Resolutions and relevant regulations and legislation on targeted financial sanctions against the financing of terrorism.

6.2 Reporting entity shall extend the suspicious transaction report mechanism to cover the financing of terrorism or property or funds or other services that is suspected to be subject to targeted financial sanctions.

6.3 Reporting entity shall maintain a record of names and particulars of terrorists in the United Nations list and any terrorists designated by the authorities of Cambodia and they shall consolidate records with the other recognized lists of designated persons. Information contained in the records shall be updated and relevant and made easily accessible to employees for the purpose of identifying suspicious transactions and freezing accounts, funds or other services.

6.4 Reporting entity shall conduct checks of the names of new and existing customers against the names in the United Nations and domestic lists of designated terrorists. If there is a name match, the reporting entity shall verify and confirm the identity of its customer. If the customer and the person listed in the records are the same person, the reporting entity shall, without delay and without prior notice, freeze the customer's property, funds or other services pursuant to the law and regulation and relevant court orders and promptly inform the CAFIU. Where reporting entity suspect that a transaction is terrorist or terrorism financing related, it shall make a suspicious transaction report to the CAFIU.

7. Foreign Branches and Subsidiaries

7.1 Reporting entity that are or are part of a financial group or reporting entity that have foreign branches or majority owned subsidiaries shall implement the group wide programs.

7.2 A group wide program shall incorporate:

a) all requirements set from point 2 to point 6 of this Directive;

b) policies and procedures for sharing information between members of the group for the purposes of undertaking CDD and ML/TF risk management;

c) provision of customer information at group level of audit, compliance and ML/TF risk management and mitigation. This provision shall be conducted for the purpose of AML/CFT; and

d) policies and procedures to maintain the confidentiality, appropriate use of the information exchanged between group members and to prevent tipping-off.

7.3 Reporting entity that have foreign branches and majority owned subsidiaries must require such branches and subsidiaries to implement AML/CFT measures that are consistent with the requirements imposed by the Law on AML/CFT and this Directive:

a) where the laws of the countries in which a foreign branches or majority owned subsidiaries of a reporting entity located are more stringent than the Law on AML/CFT and this Directive, the reporting entity shall implement the AML/CFT requirements in foreign countries when it was permitted by CAFIU.

b) where the AML/CFT requirements of the countries in which the foreign branches or majority owned subsidiaries located are less stringent than those imposed in Cambodia, reporting entity shall require the foreign branches or majority owned subsidiaries implement the AML/CFT requirements in Cambodia unless it was permitted by the laws of the countries in which their foreign branches and majority owned subsidiaries operate.

c) In the event that the laws of the countries in which a foreign branches or majority owned subsidiaries of a reporting entity do not permit the foreign branches or majority owned subsidiaries to comply with AML/CFT requirements in Cambodia, financial groups shall:

   i. devise appropriate additional measures to manage and mitigate the ML/TF risks, and

   ii. notify CAFIU.

7.4 The requirements of Article 15 of the Law on AML/CFT do not prevent confidential communications between reporting entity that are part of the same group that may be required for the implementation of point 7.2 (b) and (c) of this Directive. Reporting entity shall put in place mechanisms for sharing and using information in the same group to ensure security and confidentiality protection of information.

8. Supervisory Powers

To ensure CAFIU to perform their role and responsibilities pursuant to Article 23.2 of the Law on AML/CFT, the reporting entity shall respect the power of CAFIU as follow:

a) enter the premises of a reporting entity for the purpose of inspecting, copying or gaining possession any document or records or other information or things;

b) request a reporting entity to produce any necessary document, reports, records or others; and

c) requires management, officer or employee of a reporting entity to provide any indispensable information or assistance.



9. Sanction

Any reporting entity which do not comply with this Directive shall be penalized as stated in Article 36 and Article 37 of the Law on AML/CFT.

Up on receiving this directive, all reporting entities shall effectively implement this Directive from the date of the signature.

Phnom Penh, 11 January 2022

Cambodia Financial Intelligence Unit
Head
(Signed and Sealed)

SAY SAM ATH

Attention to:
- Office of the Council of Ministers
- National Coordination Committee on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Proliferation
- Cambodia Financial Intelligence Unit's Board of Directors
- Documentations-Archives

Directive
on
Customer Due Diligence Measures

KINGDOM OF CAMBODIA
NATION RELIGION KING

NATIONAL BANK OF CAMBODIA
Number B12 021 050 S.K.N.N

Unofficial Translation

Directive
on
Customer Due Diligence Measures

Pursuant to the Law on Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0620/021 dated 27 June 2020 the Cambodia Financial Intelligence Unit issues Directive on Customer Due Diligence measures.

1. Scope

This Directive shall apply to all reporting entity referred to in Article 4 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), including any person or profession that may be designated as a reporting entity pursuant to Article 4.15 of the AML/CFT Law.

2. Definitions

Terms used in this Directive are defined as below:

a) "Controlling ownership interest" in a legal person, for the purposes of Article 3.10 (a) of the AML/CFT Law and this Directive, shall mean a direct or indirect ownership interest of 20% or more of the shares or voting rights.

b) "Family members" shall mean individuals who are related to a Politically Exposed Person (PEP) as following:

   i. parent;

   ii. sibling;

   iii. spouse;

   iv. child; or

   v. spouse's parent.

c) "Close associate" shall mean a person who is in a position to conduct domestic and international financial transactions on behalf of a PEP. Also, a person who is publicly known to maintain a close personal, business or professional relationship with the PEP, include:

   i. financially dependent individuals (e.g. persons salaried by the PEP such as drivers, bodyguards, secretaries);

   ii. business partners or associates of the PEP;

   iii. prominent members of the same organization as the PEP;

P.O Box 25, #88 Street 102 Corner Street 19, Sangkat Wat Phnom, Khan Daun Penh, Phnom Penh, Cambodia
Phone : + 855 23 722563
Fax/Phone : + 855 23 426117

iv. individuals working closely with the PEP (e.g. work colleagues); or

v. close friends.

d) "One off or occasional transactions" shall mean transactions that are not normal and/or customary to the profile of the customer.

e) "Senior management" shall mean any person who has authority and responsibility for controlling day-to-day activities of a reporting entity or legal person and for planning, directing or overseeing the reporting entity or legal person.

3. Risk Assessment

3.1 Risk-based approach

Reporting entity shall adopt risk-based approach to identify, assess, manage, and mitigate their Money Laundering or Terrorism Financing (ML/TF) risks in accordance with Article 8.1 and 8.3 of the AML/CFT Law. The risk assessment process shall include an assessment of the following categories of risk:

a) customer risk;

b) geographic risk associated with transactions, customers, products and services, and others;

c) risks associated with individual products, services, delivery channels and/or technologies; and

d) other factors giving rise to the risk of ML/TF within or involving the reporting entity.

3.2 Record keeping and ongoing monitoring

Assessments prepared pursuant to Point 3 of this Directive shall be recorded in writing and reviewed periodically, kept up-to-date and documented. Where new products, services, delivery channels and/or technologies are introduced, the ML and TF risks associated with them shall be assessed prior to their implementation.

3.3 Bases of the risk assessment

The nature, scope, and complexity of a risk assessment prepared pursuant to Article 8.3 of the AML/CFT Law and Point 3 of this Directive shall be commensurate with the size and complexity of the reporting entity's business and ML/TF risk environment in which it operates.

4. Obligations of reporting entity

4.1 Customer Due Diligence (CDD) thresholds

4.1.1 The threshold for undertaking CDD measures required in Chapter III of the AML/CFT Law in relation to occasional or one-off transactions is 40,000,000 (forty million) Riels or foreign currency equivalent except for wire transfers or transactions involving reporting entity referred to in Article 4.10 and Article 4.13 of the AML/CFT Law.

4.1.2 The threshold for undertaking CDD measures required in Chapter III of the AML/CFT Law in relation to remittance and wire transfers are 4,000,000 (four million) Riels or foreign currency equivalent.

4.1.3 The threshold for undertaking CDD measures required in Chapter III of the AML/CFT Law in relation to reporting entity referred to in Article 4.10 of the AML/CFT Law is 60,000,000 (sixty million) Riels or foreign currency equivalent.

4.1.4 The threshold for undertaking CDD measures required in Chapter III of the AML/CFT Law in relation to reporting entity referred to in Article 4.13 of the AML/CFT Law is 12,000,000 (twelve million) Riels or foreign currency equivalent.

4.2 Measures to be taken for the identification and verification of customers of reporting entity

4.2.1 Where one or more of the conditions for undertaking CDD set out in Article 8.4 of the AML/CFT Law are satisfied, and subject to the thresholds and exceptions referred to in Point 4.1 of this Directive, reporting entity shall identify and verify their customers in accordance with Article 8 of the AML/CFT Law and this Directive.

4.2.2 Customers who are natural persons

a) Where CDD is required in relation to a natural person, reporting entity shall obtain from the customer at least the following information:

   i. full name
   ii. date of birth
   iii. identity card/passport
   iv. occupation/business
   v. nationality
   vi. address and
   vii. whether they are acting on behalf of another person.

b) The information referred to in Point 4.2.2 (a) of this Directive shall be verified the original documents, issued by the competent authorities, that contain photograph and requirements as in Point 4.2.2 (a) of this Directive.

c) Where a customer subject to CDD requirements is acting on behalf of another person, the identification and verification requirements of Point 4.2.2 (a) and (b) of this Directive shall be completed for that person.

4.2.3 Customers who are legal persons

a) Where CDD is required in relation to a legal person, reporting entity shall obtain from the customer at least the following information:

   i. registered name of the legal person

ii. date of incorporation

iii. registered number issued by incorporating authority

iv. registered office

v. address of place or places of business

vi. nature of business undertaken

vii. names and addresses of directors or partners

viii. names and addresses of shareholders and

ix. names and addresses of any person who is authorized to represent legal person or beneficial owner of legal person

b) The information referred to in Point 4.2.3 (a) of this Directive shall be verified by the original of the following documents:

i. Memorandum or article or certificate of incorporation or partnership

ii. company registration documents showing the registered office and the names of directors or partners

iii. company registration documents showing the names of shareholders

iv. any company resolution authorizing a person to represent the customer

v. any authorization or permit that has been issued that allows the customer or any person who act on behalf of beneficial owner of the customer to conduct its business.

c) Persons who are identified as the:

i. directors,

ii. partners, or

iii. shareholders, of a customer shall be identified and verified in accordance with the requirements of Point 4.2.2 of this Directive.

d) The requirements of Point 4.2.3 (a) (viii), (b) (iii) and (c) (iii) of this Directive do not apply to customers that are listed public companies.

e) Reporting entity shall conduct a basic search or enquiry on the background of such customer to ensure that it has not been, or is not in the process of being, dissolved or wound-up.

f) The identity of all account signatories shall be verified according to customer due diligence for natural person. When signatories change, care shall be taken to ensure that the identity of all current signatories has been verified.

g) To verify the information provided, reporting entity shall check with the registry of customer on the authenticity of the information provided on the

identity of customer and its directors, partner, shareholders, and any person who is authorized to represent legal person or beneficial owner of legal person.

4.2.4 Customers who are or who represent a trust or legal arrangement

a) Where CDD is required in relation to a trust or a legal arrangement or a person that represents a legal arrangement, reporting entity shall obtain from the customer at least the following information:

i. the name of the trust or legal arrangement

ii. the name of the person who is authorized to hold or deal with the property of the trust or legal arrangement (trustee)

iii. the name of the person who provided or donated the property held on behalf of the trust or legal arrangement (trustor, donor)

iv. the name of appointor who appointed the person

v. the name of the person or persons or the class of persons for whose benefit the trust or legal arrangement has been established (beneficiaries)

b) The information referred to in Point 4.2.4 (a) of this Directive shall be verified by the original of the following documents, of which copies shall be made:

i. the deed or other document that establishes the trust or legal arrangement.

ii. the deed or other document that appoints or identifies the persons referred to in Point 4.2.4 (a) (ii-v) of this Directive or any other person connected with the operation of the trust or legal arrangement.

c) Reporting entity shall require a written assurance from the person who is authorized to hold or deal with the property of the trust or legal arrangement (trustee) that evidence of the identity of the beneficiaries has been obtained, recorded and retained, and that the trust or nominee is satisfied regarding the source of funds and wealth. This assurance together with any required identification information shall be immediately available to reporting entity when requested.

4.2.5 Other requirements relating to the identification and verification of customers who are legal persons or who are or are representing trusts or legal arrangements

Where a reporting entity is in the process of establishing business relations with a legal person, or persons representing a trust or a legal arrangement, it shall take reasonable measures to understand the structure and beneficial ownership of the legal person and the property that is held on behalf of the trust or legal arrangement.

4.2.6 Customers who are a Non-Government Organization or Foundation

a) reporting entity shall require a non-government organization or foundation establishing business relationship to furnish the constitution documents or other similar documents to ensure that it is properly constituted and registered.

b) the identity of all account signatories shall be verified in accordance with the requirements of Point 4.2.2 of this Directive. When signatories change, care shall be taken to ensure that the identity of all current signatories has been verified.

c) reporting entity shall take steps to understand who is in control and makes decisions regarding the Non-government organization or foundation, and the use of the funds.

4.3 Beneficial owners

The reporting entity shall undertake additional CDD until it has identified the natural person who is the beneficial owner in accordance with the requirements of Article 8.5 (b) of the AML/CFT Law if, upon completing the identification and verification requirements set out in Point 4.2.2 - 6 of this Directive, a reporting entity is not satisfied that:

a) the customer is both the legal and beneficial owner of the customer or

b) the customer is both the legal and beneficial owner of the property that is subject of a transaction or proposed transaction with the customer.

4.4 Politically Exposed Persons (PEPs)

4.4.1 In relation to foreign PEPs, reporting entity shall undertake CDD measures required by the AML/CFT Law and Point 4.3 of this Directive and in addition they shall:

a) obtain senior management approval before establishing (or continuing, for existing customers) such relationships;

b) take reasonable measures to establish the source of funds and wealth of such persons and beneficial owners identified as PEPs;

c) ensure that enhanced, ongoing monitoring is conducted on that relationship; and

d) put risk management systems in place to identify customers or beneficial owners who are foreign PEPs.

4.4.2 In relation to domestic or international PEPs, reporting entity shall undertake CDD measures required by the AML/CFT Law and Point 4.3 of this Directive and in addition they shall:

a) take reasonable measures to determine whether a customer or beneficial owner is a domestic or international PEPs; and

b) apply enhanced, ongoing monitoring where a customer is identified as a domestic or international PEPs and the relationship is assessed as a higher risk relationship.

4.4.3 The measures referred to in Point 4.4.1 - 4.42 of this Directive shall also be applied to the family members and close associates of all PEPs.

4.5 Reliance on intermediaries or other third parties for Customer Due Diligence or introduced business

4.5.1 Reporting entity may rely on third parties to undertake CDD measures relating to the identification of the customer or beneficial owner or ownership and control structure of customer and obtaining information relevant to obtaining an understanding the nature and purpose of the business relationship. Such measures shall, at a minimum, be in accordance with the requirements of Article 8 of the AML/CFT Law and this Directive. The ultimate responsibility of CDD always remains with reporting entity.

4.5.2 Reporting entity shall ensure that a third party relied upon to undertake the CDD measures referred to in Point 4.5.1 of this Directive retains copies of identification data and any other relevant documents produced as part of the CDD process in their records, which shall be made available to the reporting entity when required without delay.

4.5.3 Reporting entity shall satisfy themselves that a third party relied upon to perform CDD measures is regulated, supervised or monitored for compliance with the FATF standards relating to CDD and record keeping in other jurisdictions.

4.5.4 Reporting entity shall not employ third parties to undertake CDD measures if they are based in jurisdictions that have been identified as posing a high level of ML/TF risk pursuant to instruction issued by CAFIU.

4.5.5 A reporting entity may rely upon a third party to conduct the CDD referred to in Point 4.5.1 of this Directive if it is part of the same financial group as the reporting entity and:

a) the group applies CDD and record keeping requirements that are in accordance with the requirements of the AML/CFT Law and this Directive;

b) the implementation of group wide CDD and record keeping requirements are supervised at group level by a competent authority; and

c) CDD processes undertaken in higher risk countries, adequately mitigate risk by the group's AML/CFT policies and controls.

4.5.6 Reporting entity shall periodically review the CDD measures undertaken by third parties.

4.6 Simplified Customer Due Diligence

4.6.1 Where a reporting entity has undertaken a written risk assessment that demonstrates that a product and service, geography, transactions, delivery channel and/or technologies, or class of customers has a low risk of ML/TF, it may apply simplified CDD measures, which are less stringent than CDD measures, in relation to that product, delivery channel and/or technologies, or class of customers.

4.6.2 Simplified CDD measures that are applied by a reporting entity shall be:

a) commensurate with the ML/TF risks identified in the risk assessment; and

b) clearly set out in writing in the reporting entity's AML/CFT procedural guidelines and manuals.

4.6.3 Given a specified commencement date referred to in Point 4.6.1 of this Directive reporting entity shall not apply simplified CDD measures whenever there is a suspicion of ML/TF, or where specific higher-risk scenarios apply.

4.7 Enhanced Customer Due Diligence (EDD)

4.7.1 Reporting entity shall conduct EDD for all categories of higher risk customers, including foreign PEPs and where other categories of risk, including geographic risk or risk associated with products, services, delivery channels and/or technologies are high to ensure that reporting entity is not abused by money launderers and financiers of terrorism.

4.7.2 All risk factors, including country or geographic risk, products and services risk and risks associated with types of transaction, delivery channel and/or technologies, such as money exchange, non-face-to-face business and relationship, private banking…etc. shall be included in determining whether a customer or transaction presents a high risk of ML or TF.

4.7.3 EDD shall include at least:

a) obtaining more detailed information from the customer, in particular, on the purpose, intended nature and reasons of the business relationship and source of funds and wealth;

b) undertaking more frequent audit and reviews of customer activity by compliance officer and auditor;

c) undertaking independent research and sourcing of additional information about the customer;

d) obtaining approval of senior management to the commencement or continuation of the business relationship; and

e) implementing monitoring and reporting mechanisms to identify potential ML/TF activities.

4.8 Ongoing Customer Due Diligence

4.8.1 Reporting entity shall conduct on-going CDD and scrutiny, to ensure the information provided is updated and relevant and ensure that the transactions being conducted are consistent with the reporting entity's knowledge of the customer, their business, ownership and control structure, and risk profile, including, where necessary, the source of funds and wealth.

4.8.2 Unwillingness of the customer to provide the information requested during initial or ongoing CDD procedures or to cooperate with reporting entity' CDD process shall be regarded as suspicious and may justify making a report pursuant to Article 12 of the AML/CFT Law.

4.9 Existing customers

4.9.1 Reporting entity shall take necessary measures to ensure that the records of existing customers remain up-to-date and relevant. Further evidence of the identity of existing customers shall, where necessary, be obtained to ensure compliance with CDD standards set by this Directive.

4.9.2 Reporting entity shall conduct regular reviews on existing records of customers. These reviews shall at least, be conducted when:

a) a significant transaction is to take place;
b) there is a material change in the way the account is operated;
c) the customer's particulars change substantially; or
d) information held on the customer is insufficient.

4.9.3 In the event that the circumstances above do not arise, reporting entity shall, based on risk assessment, obtain additional information in line with their current standards from those existing customers that are of higher risk.

4.10 Insurance

4.10.1 Reporting entity shall undertake the additional CDD measures required in this Part in addition to the measures required in the AML/CFT Law and this Directive when it establishes a relationship with a customer that involves a life insurance policy or other form of investment related insurance policy.

4.10.2 When the beneficiary of a life insurance policy or other form of investment related insurance policy is identified or designated, the reporting entity shall:

a) take the name of the beneficiary, where the beneficiary is identified as a named natural or legal person or a named legal arrangement.
b) obtain sufficient information concerning the beneficiary to enable the reporting entity to establish the identity of the beneficiary at the time of the payout, where the beneficiary is designated by characteristics or is a member of a class of persons.

4.10.3 Whichever form of identification is undertaken in accordance with Point 4.10.2 of this Directive, the verification of the identity of the beneficiary shall be undertaken prior to the payout of the life insurance policy.

4.10.4 Reporting entity shall:

a) include the beneficiary of a life insurance policy or other investment related insurance policy as a relevant risk factor in determining whether EDD shall be undertaken. If reporting entity determines that a beneficiary who is a legal person or a legal arrangement presents a higher risk, it shall take enhanced measures which include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

b) ensure that the requirements of risk assessment of this Directive are included as part of their practices and procedures.

4.11 Record keeping

4.11.1 Reporting entity shall record customer identification and domestic and international transactions including CDD measures records, transaction records, account files, business correspondence and the results of any analysis undertaken in relation to the customer, including documents associated with suspicious transaction reports for at least five years after account is closed or the business relationship is ended, or after the date of the one off or occasional transaction.

4.11.2 Where CAFIU notifies a reporting entity that records subject to preservation pursuant to Article 11 of the AML/CFT Law are subjected to an on-going investigation or suspicious transaction report submitted, they shall be retained beyond the stipulated retention period until it is confirmed by the CAFIU that such records are no longer needed.

4.11.3 Copy of documents and/or data related to reports prepared pursuant to Article 12 of the AML/CFT Law shall be retained for at least five years after the date of creation of the document or five years after the ending of the business relationship with the customer, whichever is the later.

4.11.4 Reporting entity shall retain records as mention in Point 4.8.1 of this Directive as originals or copies, or in electronic form, provided that such forms are secured and retrievable upon request and provided in an accurate and timely manner.

5. The submission of information

CAFIU may require the reporting entity to swiftly provide any or any additional documents or information or data when needed for the purpose of this Directive.

6. Sanction

Any reporting entity which do not comply with this Directive shall be penalized as stated in Article 36 and Article 37 of the AML/CFT Law.

Up on receiving this directive, all reporting entities shall effectively implement this Directive from the date of the signature.

Phnom Penh, 2021

Cambodia Financial Intelligence Unit

Head
(Signed and Sealed)

SAY SAM ATH

Attention to:
- Office of the Council of Ministers
- National Coordination Committee on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Proliferation
- Cambodia Financial Intelligence Unit's Board of Directors
- Documentations-Archives

Directive

on

the Designated Threshold for Customer Due Diligence for Casinos and Other Gambling Institutions

KINGDOM OF CAMBODIA
NATION RELIGION KING

NATIONAL BANK OF CAMBODIA

Number B12.020.352. S.K.N.N

Unofficial Translation

Directive
on
the Designated Threshold for Customer Due Diligence for Casinos and Other Gambling Institutions

Pursuant to Article 8 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0620/021 dated 27 June 2020 the Cambodia Financial Intelligence Unit issues directive on the designated threshold for customer due diligence for casinos and other gambling institutions.

The designated threshold for conducting due diligence for customer or beneficial owner who carry out a transaction with casinos and other gambling institutions as stipulated in paragraph 13 of Article 4 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism are the following:

- When a customer or beneficial owner carries out a transaction with an amount equal to or above 12,000,000 (twelve million) Riels or foreign currency equivalent.

- This transaction includes several transactions of a customer or beneficial owner within 24 hours, where the total amount of the combined transactions equal to or above 12,000,000 (twelve million) Riels or foreign currency equivalent.

Any casinos and other gambling institutions which do not comply with this directive will be penalized as stated in Article 36 and Article 37 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism.

Upon receiving this directive, all casinos and gambling institutions shall effectively implement this directive from the date of the signature.

Phnom Penh, 10 November 2020

Cambodia Financial Intelligence Unit

Head

(Signed and Sealed)

SAY SAM ATH

Receiving places:
- Office of the Council of Ministers
- Ministry of Economy and Finance
- National Bank of Cambodia
- National Coordination Committee on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Proliferation
- Cambodia Financial Intelligence Unit's Board of Directors
- All casinos and gambling institutions
- Documentations-Archives

P.O Box 25,#88 Street 102 Corner Street 19, Sangkat Wat Phnom, Khan Daun Penh, Phnom Penh, Cambodia
Phone : + 855 23 722563
Fax/Phone : + 855 23 426117

Directive
on
Risk Based Supervision

KINGDOM OF CAMBODIA

NATION RELIGION KING

Cambodia Financial Intelligence Unit

N° ...B12. 020. 268 S.I.K.N.N...

Directive

On

Risk Based Supervision

Unofficial Translation

Pursuant to the law on Anti-Money Laundering and Combating the Financing of Terrorism promulgated by the Royal Kram No. NS/RKM/0620/021 dated on 27 June 2020 the Cambodia Financial Intelligence Unit (CAFIU) issues Directive on Risk Based Supervision (RBS).

1. Scope

This Directive shall apply risk-based supervision conducted by supervisor of CAFIU, hereafter called "supervisor" on reporting entity referred to Article 4 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT).

The Implementation of RBS

1.1 The supervisor shall apply RBS which refers to detection, identification, assessment, and understanding of the ML/CFT risk of each reporting entity and use the appropriate measures to prevent, manage, mitigant risks which is based on the materiality and risk as well as on going continue to enhance the effectiveness of supervision of CAFIU.

1.2 Based on the RBS, supervisor shall determine and allocate resources and develop the plan and strategy for supervision in accordance with the level of risk identified. The supervisor shall follow up and update the risk profile of individual reporting entity on quarterly basis to ensure that the risk assessment shall be appropriate, targeting and effective through at least, the development of supervisory strategies and onsite examination plan, the use of appropriate supervision approach, and the change of nature, frequency, intensity, and focus of supervision.

1.3 The supervisor shall apply, at minimum, two supervision tools including off-site tools and on-site tools and off-site tools in the process of RBS.

1.4 In the part of support of off-site tools, the supervisor shall apply:

a) Collect the documents, reports, and relevant information of the reporting entity

b) Determine the ML/FT risk levels and its changes of individual reporting entity by using Risk Based Supervision tools as in appendix and other tools developed by CAFIU.

P.O. Box 67 #22-24 Preah Norodom Blvd, Phnom Penh, Cambodia www.nbc.org.kh/cafiu cafiu_info@nbc.org.kh

c) Determine the remedial actions based on the findings of supervision to manage and mitigant the identified risk of the reporting entity, if any

d) Propose to impose sanction against any reporting entity who has insufficient measures to prevent or mitigant or manage risk identified, if any

1.5 The process of on-site supervision, supervisor shall determine the nature, scope, frequency, intensity and duration of supervision based on following criteria:

a) The result of risk assessment of individual reporting entity given by CAFIU's RBS tools

b) The result of AML/CFT risk assessment undertaken by reporting entity

c) The progress of implementation of the recommended actions in the previous on-site report, if any

d) Other information or reports related to the reporting entity.

1.6 Based on the finding of on-site examination, the examiner shall:

a) Determine the remedial actions to be taken by reporting entity

b) Propose to impose sanction against any reporting entity who has insufficient measures to prevent or mitigant or manage risk identified or did not comply with law and regulations, if any.

1.7 The supervisor shall enhance the effectiveness of supervisory activities through domestic and international cooperation.

3. Implementation

Up on receiving this directive, all CAFIU's officials, and reporting entities shall effectively implement this Directive from the date of the signature.

Phnom Penh, 12 August 2020

Cambodia Financial Intelligence Unit
Head
(Signed and Sealed)

SAY SAM ATH

Attention to:
- Office of the Council of Ministers
- National Coordination Committee on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Proliferation
- Cambodia Financial Intelligence Unit's Board of Directors
- Documentations-Archives

© ឆ្នាំ២០២៣
មិនអនុញ្ញាតឱ្យផលិតឡើងវិញ ឬបកប្រែសៀវភៅនេះដោយគ្មានការអនុញ្ញាតជាមុនជាលាយលក្ខណ៍អក្សរឡើយ។
ការផលិតឡើងវិញទាំងស្រុង ឬមួយផ្នែកនៃសៀវភៅនេះត្រូវស្នើសុំការអនុញ្ញាតពី៖
អង្គភាពស៊ើបការណ៍ហិរញ្ញវត្ថុកម្ពុជា
សារអេឡិចត្រូនិច៖ cafiu_info@nbc.gov.kh
ទូរសព្ទ៖ +855 23 427 933
គេហទំព័រ៖ cafiu.nbc.gov.kh

© 2023
No reproduction or translation of this publication may be made without prior written permission.
Applications for permission to reproduce all or part of this publication should be made to:
Cambodia Financial Intelligence Unit
Email: cafiu_info@nbc.gov.kh
Tel: +855 23 427 933
Website: cafiu.nbc.gov.kh

អង្គភាពស៊ើបការណ៍បិរញ្ញវត្ថុកម្ពុជា

សារអេឡិចត្រូនិច៖ cafiu_info@nbc.gov.kh

ទូរស័ព្ទ៖+855 23 427 933

គេហទំព័រ៖ cafiu.nbc.gov.kh