Unofficial Translation

KINGDOM OF CAMBODIA

NATION RELIGION KING

Prakas
on
Anti- Money Laundering and Combating the Financing of Terrorism relating to All Reporting Entities not regulated by the National Bank of Cambodia

Governor of the National Bank of Cambodia and
Chairman of Board of Director of Cambodia Financial Intelligence Unit

- With reference to the Constitution of the Kingdom of Cambodia
- With reference to Royal Kram No NS/RKM/0196/27 of January 26, 1996, promulgating the law on the Organization and Function of the National Bank of Cambodia
- With reference to Royal Kram No NS/RKM/1206/036 of December 29, 2006, promulgating the law on Amendment Article 14 and Article 57 of the Law on the Organization and Function of the National Bank of Cambodia
- With reference to Royal Kram N° NS/RKM/0607/014 of June 24, 2007, promulgating the Law on Anti-Money Laundering and Combating Financing of Terrorism
- With reference to the Royal Decree NS/RKT/0508/526 of May 13, 2008 on the appointment of His Excellency Chea Chanto as General Governor of the National Bank of Cambodia, which is equivalent to Senior Minister
- With reference to Sub Decree 95 RNKR/TT of February 01, 2008 on the appointment of His Excellency Chea Chanto as a chairman of Board of Directors of Cambodia Financial Intelligence Unit
- Pursuant to the request of the Secretariat of Cambodia Financial Intelligence Unit
- Pursuant of the spirit of the 9th Board of Director Meeting of Cambodia Financial Intelligence Unit dated December 07, 2010.

Decides

Article 1 – Scope

For the purposes of the present Prakas the term “reporting entities” shall apply to the following institutions and professions, which are not regulated by the National Bank of Cambodia and are referred to as “reporting entities” in the *Law on Anti Money Laundering and Combating the Financing of Terrorism*:

a) non-bank financial institutions, including securities brokerage firms and insurance companies;

b) investment and pension funds, investment companies and companies for managing investment funds;

c) real estate agents, buildings and land;

d) post office operating payment transactions;

e) lawyers, notaries, accountants, auditors, investment advisors and asset managers when they prepare for or carry out transactions for their clients concerning the activities listed in Article 2 of the present Prakas;

f) casinos and other gambling institutions;

g) Non-governmental organizations and foundations engaging in business activities and fund raising;

h) Trust companies and other service provider companies

i) Any other institution or profession that is designated by the CAFIU to fall within the scope of the *Law on Anti-Money Laundering and Combating the Financing of Terrorism* and is not supervised by the National Bank of Cambodia.

Article 2 – Business Activities of Reporting Entity

When lawyers, notaries, accountants, auditors, investment advisors and asset managers prepare for or carry out transactions for a client in relation to the following activities:

a. Buying and selling real estate, buildings and land;

b. Managing of client money, securities or other assets;
   - management of banking or securities accounts;
   - organization of contributions for the creation, operation or companies management.

c. Creation, operation or management of legal persons or arrangements, and buying and selling of business entities;

d. When Trust or Company Service Providers prepare for or carry out transactions for a client concerning the following activities:
   - acting as a formation agent of legal persons;
   - acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
   - providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement;
   - acting as or arranging for another person to act as a trustee of an express trust
   - acting as or arranging for another person to act as a nominee shareholder for another person.

Article 3 – Customer Acceptance Policy

Reporting entities should develop customer acceptance policies and procedures and should have reasonable measures, including risk profile, in their internal policy and procedures to address different risks posed by each type of customer or by each individual customer.

Article 4 – Risk Profiling

4.1 In creating the risk profile of a type of customer or an individual customer, reporting entities should at least take into consideration the following factors:

- the origin of the customer and location of business;
- background and personal particulars of the customer
- nature of the customer's business;
- structure of ownership for a corporate customer; and
- any other information indicating the customer is of higher risk

4.2 Following the initial acceptance of the customer, reporting entities should continuously monitor the customer's account activity pattern to ensure it is in line with the customer profile. Unjustified and unreasonable differences should cause reporting entities to reassess the customer as higher risk.

Article 5 – Prohibition of Anonymous Account and Accounts in Fictitious Names

Reporting entities should ensure that an account is opened and maintained in the name of the account holder at all times. In addition, reporting entities should establish customer identity as outlined in articles 7 and 8 of the present Prakas to ensure that no customer is allowed to open or operate an anonymous account or an account in a fictitious, false or incorrect name.

Article 6 – Customer Due Diligence

6.1 Reporting entities must conduct customer due diligence and obtain satisfactory evidence and properly establish in its records the identity and legal existence of persons applying to do business with them. Such evidence must be substantiated by reliable documents.

6.2 The customer due diligence should be conducted, when:

- establishing business relationship with the customer such as opening an account, granting a safe deposit facility or engaging in any other business dealings;
- carrying out an occasional or one off transaction, that involves a sum in excess of 40 million Riel (40,000,000KHR) or Ten thousand USD (USD10,000 or foreign currency equivalent) or wire-transfer in excess of 4 million Riel (4,000,000KHR) or One thousand USD (USD1,000 or foreign currency equivalent)

- Cashing out the wining in gambling in excess of 40 million Riel (40,000,000KHR) or Ten thousand USD (USD10,000 or foreign currency equivalent).
- reporting entities have any suspicion of money laundering or financing of terrorism; or
- reporting entities have any doubts about the veracity or adequacy of previously obtained information.

6.3 The customer due diligence undertaken by reporting entities should at least comprise the following:

- identify the customer and verify the identity of the customer using reliable, independent source documents, data or information referred to in articles 8 or 9;
- determine if the customer conducting business is acting on behalf of another person or beneficial owner;
- understanding the beneficial ownership and control structure of the customer. Beneficial owner is defined in article 09 of the present Prakas;
- conduct on-going due diligence 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 and risk profile, including, where necessary, the source of funds.

6.4 Unwillingness of the customer to provide the information requested and to cooperate with reporting entities' customer due diligence process may itself be a factor of suspicion.

6.5 Reporting entities should not open the account, commence business relations or perform transaction, or in the case of existing business relations with customers, it should terminate such business relations if the customer fails to comply with the customer due diligence requirements. Such situation warrants a suspicious transaction report to be submitted to the CAFIU.

Article 7 – Individual Customers

7.1 In establishing a business relationship with an individual customer, reporting entities should obtain from the individual customer at least the full name, date of birth, identity card/passport number/identity document reference number, occupation/business, nationality and address.

7.2 Reporting entities should require the individual to furnish the original and make copies of one or more of the following documents:

- National identity card;
- Passport; or
- Identity documents preferably bearing a photograph of the customer, issued by an official authority.
-

Article 8 – Corporate Customers

8.1 In establishing a business relationship with a corporate customer, reporting entities should require the company/business to furnish the original and make copies of at least the following documents:

- Memorandum/Article/Certificate of Incorporation/Partnership
- Identification document of Board of Director/Directors/Shareholders/Partners
- Board of Directors'/Directors' Resolution
- Authorisation for any person to represent the company/business
- Authorisation or permit to conduct business

8.2 In addition, reporting entities should conduct a basic search or enquiry on the background of such company/business to ensure that it has not been, or is not in the process of being, dissolved or wound-up.

8.3 The identity of all account signatories shall be verified according to customer due diligence for individual customers. When signatories change, care should be taken to ensure that the identity of all current signatories has been verified.

8.4 To verify the information provided, reporting entities should check with the Registry of Companies/Businesses on the authenticity of the information provided on the identity of the company/business and its directors, owners, shareholders and office bearers.

8.5 Where the customer or the owner of the controlling interest is a public company that is subject to regulatory disclosure requirements i.e. a public company listed on a recognised stock exchange, it is not necessary to seek to identify and verify the identity of the shareholders of that public company.

8.6 Reporting entities should also understand the ownership and control structure of corporate customers and determine the source of funds of the company/business. This will assist reporting entities in ascertaining any suspicion concerning the changes to the ownership or control structure and in developing the customer profile and expected activity through the company/business account.

Article 9 – Beneficial Owner

Reporting entities should conduct customer due diligence as stringent as the one imposed on individual customer when they suspect a transaction is conducted on behalf of a beneficial owner in addition to the customer who is conducting such transaction. Beneficial owner is the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

Article 10 – Non-Government Organization and Foundation

10.1 Reporting entities should 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.

10.2 The identity of all account signatories shall be verified according to customer due diligence for individual customers. When signatories change, care should be taken to ensure that the identity of all current signatories has been verified.

10.3 Reporting entities should take steps to understand who is in control and makes decisions regarding the Non-government organization/foundation, and the use of the funds.

Article 11 – Trust and Nominee Accounts

11.1 Reporting entities need to establish whether the customer is acting on behalf of another person as trustee, nominee or agent.

11.2 Reporting entities should take reasonable measures to understand the ownership and control structures and the relationship among the relevant parties in handling a trust or nominee account and obtain evidence of the identity of the settler, trustee, nominee, authorised signatories, persons exercising effective control and the beneficiaries.

11.3 Reporting entities should ensure customer due diligence requirements are completed for beneficial owners, when the trust or nominee account is established.

11.4 Reporting entities require a written assurance from the trust or nominee 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. In addition, identification information must be immediately available to reporting entities upon request.

Article 12 – Client Accounts

Reporting entities should satisfy themselves about transactions passing through lawyers and accountants clients' accounts that give cause for concern, and should report those transactions to CAFIU, if any suspicion is aroused.

Article 13 – Shell Companies

Reporting entities should not open an account for or conduct business with a shell company, which do not conduct any commercial activities or have any form of commercial presence in the country but are legal entities through which financial transactions may be conducted.

Article 14 – Reliance on Intermediaries or Other Third Parties for CDD or Introduced Business

14.1 Reporting entities should be wary and ensure that they do not fall complacent and completely rely on the customer due diligence conducted by the intermediaries or other third parties they use. The ultimate responsibility of customer due diligence always remains with reporting entities.

14.2 Reporting entities must be satisfied that the introducing intermediary:

- has carried out customer due diligence by identifying the customer and verify that identity using reliable, independent source documents, data or information;
- has identified the beneficial owner and in respect of corporate customers understands the ownership and control structure of the customer;
- understands the purpose and nature of the business relationship;
- has put in place a system to provide the reporting entity with access to the identification documents, data or information upon request and without delay;
- allows periodic review by reporting entities to verify the due diligence undertaken; and
- is properly regulated and supervised for AML/CFT purposes by the respective authority.

Article 15 – Non Face-to-Face Customers

15.1 Reporting entities should pay special attention in establishing and conducting non-face-to-face business relationships and undertake customer due diligence through face-to-face interaction, or through an intermediary as required by article 14 of the present Prakas, prior to establishing such business relationships with their customers.

15.2 Reporting entities are also required to implement monitoring and reporting mechanisms to identify potential money laundering and financing of terrorism activities.

Article 16 – Politically Exposed Persons (PEPs)

16.1 Reporting entities should check current and new customers to determine whether they are Politically Exposed Persons, as defined in article 3 of the Law on Anti-Money Laundering and Combating the Financing of Terrorism, as part of the customer due diligence process. Reporting entities should gather sufficient information from the said customer and research further data or information to determine the level of AML/CFT risk.

16.2 Once a PEP is identified, reporting entities should take reasonable measures to establish the source of wealth and funds of such persons.

16.3 The decisions to enter into or continue business relationships with these PEPs should be made by the senior management of reporting entities.

16.4 Reporting entities should develop a risk profile of each PEP based on information collected from the customer and obtained through independent research and understand the full nature of the business relationship and transaction activity. There should be on-going monitoring of the relationship and activity against the risk profile and any concerns arising from the monitoring process should be reported to senior management and, if appropriate, also reported to the CAFIU.

Article 17 – Other Higher Risk Customers

17.1 Reporting entities shall conduct enhanced customer due diligence for all categories of higher risk customers, including PEPs to ensure that reporting entities are not abused by money launderers and financiers of terrorism.

17.2 Enhanced due diligence should include at least:

- more detailed information from the customer, in particular, on the purpose of the business relationship and source of funds;
- independent research and sourcing of additional information about the customer; and
- approval by senior management.

Article 18 – Existing Accounts

18.1 Reporting entities should 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 should, where necessary, be obtained to ensure compliance with customer due diligence standards set by the present Prakas

18.2 Reporting entities should conduct regular reviews on existing records of customers. These reviews should at least, be conducted when:

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

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

Article 19 – Record keeping

19.1 Reporting entities should keep all records, documents and copies of documents involved in all forms of transactions for at least 5 years after the date of the transaction. All identification data, files, records, documents, business correspondence and copies of documents obtained on a customer must be maintained for at least 5 years after the accounts have been closed or the business relations with the customer have ended.

19.2 Where the records 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 relevant authority that such records are no longer needed.

Article 20 – Audit Trail

20.1 Reporting entities must ensure that the retained documents and records are able to create an audit trail on individual transactions that would enable the supervisory and enforcement agencies to trace funds.

20.2 The records kept must enable reporting entities to establish the history and nature of and reconstruct each transaction. The records shall include at least:

- the origin of funds, such as method of receipt and or name of originator of wire transfer;
- the identity of the person undertaking the transaction if not an account holder;
- the type of transaction; and
- the instruction and the destination of fund transfers.

Article 21 – Record Format

Reporting entities should retain the relevant document as originals or copies, on microfilm or in electronic form, provided that such forms are secured and retrievable upon request and provided in an accurate and timely manner

Article 22 – On-Going Monitoring

22.1 Reporting entities should conduct on-going due diligence for all customer relationships, using a risk-based approach. The risk-based approach to on-going customer due diligence should ensure that the risk profile of the customer is up-to date.

22.2 Reporting entities shall pay special attention to all complex, unusual large transactions, or unusual patterns of transactions, to determine whether the transactions have an apparent or visible or lawful purpose.

Article 23 – Management Information System

Reporting entities should put in place an adequate management information system for identifying and detecting transactions that they suspect or have reasonable grounds to suspect related to proceeds from an unlawful activity or the customer is involved in money laundering or financing of terrorism. The management information systems should provide reporting entities timely information on a regular basis to enable them to detect suspicious activity.

Article 24 – Special Attention

Reporting entities should conduct on-going due diligence with regards to business relationships and transactions with individual, business, company and financial institution from countries which have insufficiently implemented the internationally accepted AML/CFT measures. Such business relationships and transactions should require reporting entities to make further detailed inquiries, about their background and purpose, to establish the findings in writing, and to make them available to the competent authorities.

Article 25 – Cash Transaction Reporting

25.1 Reporting entities are required to report to the CAFIU cash transactions of or exceeding 40 Million Riels (40,000,000R) or foreign currency equivalent.

25.2 Cash transaction reports shall be provided to the CAFIU, within 14 days of the date of the transaction and be submitted on the approved 'Cash Transaction Report' form issued by the CAFIU or using the approved format for electronic reporting. CAFIU shall provide reporting entities with a copy of the approved Cash Transaction Report form.

25.3 Reportable cash transactions include multiple cash transactions for a customer / account where the total amount of the combined transactions or total winning cash out of or exceeds 40 Million Riels (40,000,000R) or foreign currency equivalent in any one day.

Article 26 – Suspicious Transaction Reporting

26.1 Reporting entities are required to establish a reporting system and to promptly submit suspicious transaction reports to the CAFIU when any of its employee suspects or has reasonable ground to suspect that the transaction involves proceeds of an offence or are related to money laundering or financing of terrorism or they have any other ground of suspicion about a customer transaction. Reporting entities should establish their own internal guidelines on suspicious transaction reporting incorporating the relevant provisions in the Law on Anti Money Laundering and Combating the Financing of Terrorism, the relevant provisions in the present Prakas and any suspicious transaction indicators listed in guidelines issued by the CAFIU.

26.2 Reporting entities should also submit a suspicious transaction report when a new or existing customer fails to complete the customer due diligence without reasonable excuse, regardless of whether the reporting entity accepts, rejects, continues or terminates the business relationship with such customer.

Article 27 – Reporting Mechanisms

27.1 Reporting entities should appoint an officer at the senior management level to be the compliance officer responsible for the submission of suspicious transaction reports to the CAFIU. The appointed compliance officer should be the point of reference for the CAFIU and reporting entity. Reporting entities should ensure that all suspicious transaction reports prepared by employees are properly channelled to the compliance officer.

27.2 The employees of reporting entities should report suspicious transactions to the compliance officer even if they do not know precisely what the underlying unlawful activity is or whether such activities have occurred.

27.3 Once the suspicious transaction report reaches the compliance officer, the compliance officer should promptly evaluate and establish whether there are reasonable grounds for suspicion and promptly, within 24 hours, submit the suspicious transaction report to the CAFIU unless the compliance officer considers, and records his/her opinion, that such reasonable grounds do not exist.

27.4 The suspicious transaction report submitted by the compliance officer shall be in writing and using the approved form available from the CAFIU and delivered by safe hand, secured mail or secured electronic transmission to CAFIU.

27.5 Reporting entities should ensure that when preparing and submitting a suspicious transaction report, information about the suspicious transaction, the customer and the reporting of the matter remains confidential and is available only to staff, on a strict 'need to know' basis.

27.6 Reporting entities should authorise their compliance officer to cooperate with the CAFIU in providing additional information and documentation requested and to address further enquiries with regard to the submitted suspicious transaction report.

Article 28 – Prohibition of Tipping Off

28.1 Reporting entities must ensure that the reporting system put in place for the submission of suspicious transaction reports is operated in a confidential manner.

28.2 Reporting entities must ensure that the customer reported on, is not informed of the existence of the suspicious transaction report or does not become aware of such suspicious transaction report. Staff should be made aware that article 15 of the Law on Anti Money Laundering and Combating the Financing of Terrorism prohibits any individual having knowledge of a suspicious transaction report from communicating such information or reports to any natural or legal persons other than the CAFIU, except where so authorized by the CAFIU.

Article 29 – Others Issues

29.1 Reporting entities should maintain a complete file on all suspicious transaction reports submitted by their employees to its compliance officer and such reports that have been further submitted to the CAFIU.

29.2 Reporting entities must take reasonable measures to ensure that all their officers and employees involved in conducting or facilitating customer transactions are aware of these reporting procedures.

Article 30 – Detection and Reporting of the Financing of Terrorism

30.1 Reporting entities should take the necessary measures to ensure compliance with the United Nations Security Council (UNSC) Resolutions and relevant regulations and legislation on financing of terrorism.

30.2 Reporting entities should extend the suspicious transaction report system and mechanism to cover suspicion of financing of terrorism.

30.3 Reporting entities should maintain a record of names and particulars of terrorists in the United Nations list and they should consolidate records with the other recognised lists of designated persons. Information contained in the records should be updated and relevant and made easily accessible to employees for the purpose of identifying suspicious transactions and freezing accounts / funds.

30.4 Reporting entities should conduct checks of the names of new and existing customers against the names in the records. If there is a name match, the reporting entities should take reasonable measures to 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 should immediately freeze the customer's funds / assets

and inform the CAFIU. Where reporting entities suspect that a transaction is terrorist-related, it should make a suspicious transaction reports to the CAFIU.

Article 31 – Risk Management

31.1 The Board of Directors of reporting entities should establish an effective internal control system for AML/CFT compliant with legal and regulatory requirements. It is the responsibility of the senior management to ensure such internal controls are implemented effectively.

31.2 The Board of Directors and senior management should be aware of and understand the AML/CFT measures required by law, regulations, the industry's standards and best practices as well as the importance of putting in place AML/CFT measures to prevent their reporting entity from being abused by money launderers and financiers of terrorism. The Board of Directors should oversight the overall AML/CFT measures undertaken by the reporting entity.

31.3 The Board of Directors and senior management should be aware of the money laundering and financing of terrorism risks associated with all its business products and services.

31.4 The Board of Directors should ensure that its reporting entity has, at the minimum, policies on AML/CFT procedures and controls. The senior management should assist the Board of Directors in formulating the policies and ensure that the policies are in line with the risks associated with the nature of business, and complexity and volume of the transactions undertaken by the reporting entity.

31.5 The Board of Directors should ensure that the procedures for AML/CFT measures including those required for customer acceptance policy, customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are in place.

31.6 The Board of Directors should assess the implementation of approved AML/CFT policies by the senior management via periodic reports.

31.7 The Board of Directors should define the lines of authority and responsibilities for implementing the AML/CFT measures and ensure that there is a separation of duty between those implementing the policies and procedures and those enforcing the controls. The Board of Directors should ensure the:

- appointment of a compliance officer to ensure that the policies, procedures and controls are in place; and
- effectiveness of internal audit in assessing and evaluating the controls in place to counter money laundering and financing of terrorism.

31.8 The Board of Directors should review and assess the policies and procedures on the AML/CFT measures in line with changes and developments in its products, services and technology systems, as well as trends in money laundering and financing of terrorism techniques. The senior management should implement the necessary changes to the policies and procedures with the approval of the Board of Directors to ensure that the current policies are sound and appropriate.

31.9 The Board of Directors and senior management should ensure that there are adequate ongoing AML/CFT training programs in place.

Article 32 – Staff Integrity

Senior management should ensure that its reporting entity establish an employee assessment system, approved by the Board of Directors, to adequately screen its employees, both existing and new, to ensure that the integrity of its employees is not compromised. The employee assessment system should at least examine personal information including criminal records, employment and financial history of its new employees as part of the recruitment process.

Article 33 – Compliance Officer

33.1 Senior management is responsible to appoint the compliance officer at the senior management level with the approval of the Board of Directors. Senior management should ensure that the compliance officer effectively discharges his/her AML/CFT responsibilities. The compliance officer should act as the reference point for the AML/CFT measures the reporting entity has established, including employee training and reporting of suspicious transactions.

33.2 Reporting entities should upon the appointment or change in the appointment of the compliance officer inform the CAFIU of the details of the compliance officer including the name, address, telephone number, facsimile number, e-mail address and other relevant background.

33.3 Reporting entities should 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:

- implementation of the policies for AML/CFT measures;
- the appropriate AML/CFT procedures including customer acceptance policy, customer due diligence, record keeping, on-going monitoring, reporting of suspicious transactions and combating the financing of terrorism are implemented effectively;
- regular assessment of the AML/CFT mechanisms to ensure that the mechanisms are sufficient to address the changing trends;
- the channel of communication from the respective employees to the compliance officer is secured and that any information is kept confidential;
- compliance with the AML/CFT legal and regulatory requirements;
- all employees are aware of AML/CFT measures including policies, control mechanisms and channels of reporting to ensure the effectiveness of such measures;
- the identification of money laundering and financing of terrorism risks associated with new products or services or arising from the reporting entity's operational changes, including the introduction of new technology and processes.

33.4 Compliance officers should have necessary knowledge and expertise to effectively discharge his/her responsibilities, including knowledge on AML/CFT

obligations required under the relevant laws and regulations and an understanding of developments in money laundering and financing of terrorism techniques

Article 34 – Staff Training and Awareness Programmes

34.1 Reporting entities should have an awareness and training programme on AML/CFT practices and measures for their employees. The training and awareness programme must be extended to all new and existing employees.

34.2 Senior management should ensure that proper channels of communication are in place to inform all levels of employees in reporting entities of their AML/CFT policies and procedures.

34.3 Employees should be aware of AML/CFT policies and controls in place and the requirements as specified in the present Prakas and in reporting entities AML/CFT internal manual.

34.4 The AML/CFT internal manual should at least contain the following:

- the *Law on Anti-Money Laundering and Combating the Financing of Terrorism*;
- the present Prakas ;
- the FATF Forty plus Nine Recommendations;
- the reporting entity's measures to meet all AML/CFT requirements.

34.5 Reporting entities should at least adapt to their needs the following training packages for the various sectors of employees within their institutions:

❖ *New Employees:*

A general background to money laundering and financing of terrorism, the requirement and obligation to identify and report suspicious transactions to the appropriate designated point within reporting entities, and the importance of not tipping off the customer.

❖ *Front-Line Employees:*

Employees who deal directly with the customers as the first point of contact with potential money launderers and financiers of terrorism should be trained in identifying suspicious transactions, measures to be taken once a transaction is deemed to be suspicious, factors that may give rise to suspicions, large cash reporting and enhanced customer due diligence.

❖ *Employees - Account Opening/New Customers:*

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

❖ *Supervisors and Managers:*
Supervisors and managers should receive a higher level of instruction covering all aspects of AML/CFT procedures including the penalties for non-compliance to the AML/CFT requirement, and procedures in addressing combating the financing of terrorism issues.

34.6 These training and awareness programmes should be conducted regularly with refresher courses provided for employees. New employees should be trained within three months of commencement of employment and front line employees, supervisors and managers should have refresher training annually.

Article 35 – Internal Audit

35.1 The Board of Directors should ensure that internal auditors undertake audit of the effectiveness and compliance with AML/CFT requirements of the relevant laws and regulations as well as the present Prakas.

35.2 The Board of Directors should ensure that the roles and responsibilities of the internal auditor are clearly defined and documented and at least include:

- testing the effectiveness of the policies, procedures and control for AML/CFT measures;
- ensuring effectiveness of AML/CFT control mechanisms including the appointment of compliance officer, staff training and awareness programmes, employee screening mechanisms and AML/CFT internal manual; and
- ensuring that measures in place are in line with current developments and changes of the relevant AML/CFT requirements.

35.3 Reporting entities should inform the CAFIU on the appointment or change in the appointment of the internal auditor and on the approach and procedures adopted by the internal auditors.

35.4 The internal auditor should submit a written report on the audit findings to the Board of Directors on a regular basis. The annual audit report should highlight inadequacies of any AML/CFT measures and control systems within the reporting entity, and the Board of Directors should ensure that necessary steps are taken to rectify the situation. Audit findings and reports on AML/CFT should be submitted to the CAFIU after consideration by the Board of Directors.

Article 36 –

The CAFIU and all reporting entities are required to implement and administer this Prakas from the date of signature.

Places:
- As article 36 for implementation
- Documentations

Copies:
- All members of Board of Director
- Ministry of Interior, Ministry of Justice, Ministry of Economy and Finance, Ministry of Commerce, Ministry of Foreign Affair and International Cooperation and Ministry of Telecommunication
- Office of the Council of Minister "for information"
- Administration Department of CM "for publication in the National Gazette"

Phnom Penh, 21 December 2010

Governor of the National Bank of Cambodia and
Chairman of Board of Directors of
Cambodia Financial Intelligence Unit