September 20, 2022

HON. DENNIS B. FUNA
Insurance Commissioner
INSURANCE COMMISSION
1071 United Nations Ave.,
Manila

Attn. : ATTY. ALBERT LAWRENCE VINZON
Division Manager
Anti-Money Laundering Division

Re : Circular Letter No. 2019-65 (November 22, 2019) in relation to AMLC Regulatory Issuance (ARI) A, B, and C, No. 2 s. 2018 and AMLC Regulatory Issuance (ARI) No. 6 s. 2021

Dear Sir:

In compliance with aforementioned Circular Letter and Regulatory Issuances, we are submitting our company's updated "Money Laundering and Terrorism Financing Prevention Program".

Thank you and hope you will find the same in order.

Very truly yours,

LOURDES M. CORCELLES
Senior Vice President
lmcorcelles@cic.com.ph

INSURANCE COMMISSION
ADMINISTRATIVE DIVISION
RECORDS SECTION
RECEIVED
SEP 20 2022
By: Time:

COMMONWEALTH INSURANCE COMPANY (CIC)

MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION PROGRAM

(As of September 2022)

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

I. Policy Statement
II. Scope
III. Definition of Terms and Abbreviations
IV. Basic Principles and Policies to Combat Money Laundering and Terrorist Financing
A. Customer Acceptance Policy
B. Compliance with Laws and Regulations
C. Cooperation with Regulatory and Law Enforcement Agencies
D. Adoption of Policies and Procedures
E. Training on Anti-Money Laundering

CHAPTER 2: POLICIES, PROCEDURES AND CONTROLS

I. Insured Acceptance Policy
II. Classification of Insured and Description
III. Assessment
1.) Insured Assessment Procedure
2.) Risk Assessment
IV. Customer Identification, Customer Due Diligence and Standard
1.) Customer Identification
2.) Customer Due Diligence and Standard
V. Customer Risk Profiling
VI. Diligence Required
VII. Customer Verification, CDD Measures, & Tipping Off
VIII. Employee Screening

CHAPTER 3: IMPLEMENTATION AND MONITORING (Ongoing & Manual)

I. Implementation of Money Laundering and Terrorism Financing Prevention Program (MTPP)
II. Implementation of Targeted Financial Sanctions
III. Ongoing Monitoring
IV. Manual Monitoring

CHAPTER 4: RECORDS KEEPING MANAGEMENT, RETENTION and REQUIREMENTS

I. Record Keeping
II. Safekeeping of Insurance Policies and Documents
III. Forms of Record

CHAPTER 5: DETECTION OF SUSPICIOUS TRANSACTIONS

CHAPTER 6: RISK MANAGEMENT

I. Active Board and Senior Management oversight
II. Acceptable policies and procedures embodied in a Money Laundering and Terrorist Financing Prevention
III. Appropriate Monitoring and Management Information System
IV. Periodic Audit

CHAPTER 7: CONTINUING EDUCATION AND TRAINING PROGRAM

CHAPTER -1
INTRODUCTION

I. POLICY STATEMENT:

CIC adopts this policy of the State under RA No. 10167 and 10168, otherwise known as Anti-Money Laundering Act (AMLA), as amended and the Terrorism Financing Prevention and Suppression Act, also referred to as TF Suppression Act to protect the integrity and confidentiality of its accounts and to ensure that the Philippines in general and this institution shall not be used respectively as a money laundering site and conduit for the proceeds of an unlawful activity as hereto defined. CIC further supports the State's policy to protect the life, liberty and property from acts of terrorism and takes zero tolerance approach against terrorism and to those who support and finance it and reinforce the fight against terrorism by applying relevant laws to counter financing of terrorism and related offenses in the insurance industry.

II. SCOPE:

This ICRE's Manual shall apply to CIC clients, insured and/or assured and its existing and future branches, regional offices, including agencies supervised and regulated by the I.C. under existing regulations and issuances. The scope of the money laundering prevention program shall also extend to combat terrorist financing activities.

III. DEFINITION OF TERMS AND ABBREVIATIONS:

A. **Terminologies:**

1. AMLA – Anti-Money Laundering Act, or R.A. 9160, as amended by R.A. Nos. 9194, 10167, 10365 and 10927
2. RIRR – Revised Implementing Rules and Regulations
3. MLPP or the Manual – Money Laundering and Terrorist Financing Prevention Program
4. AMLC – Anti-Money Laundering Council
5. CTF/MTPP – Counter Terrorism Financing/Money Laundering & Terrorism Financing Prevention Program
6. KYC – Know Your Customer/Client
7. CDD – Customer Due Diligence
8. RDD – Reduced Due Diligence
9. EDD – Enhanced Due Diligence
11. CAF – Client Assessment Form
12. KYCRF – Know Your Customer Reliance Form
13. PEP – Politically Exposed Person
14. BSP – Bangko Sentral ng Pilipinas
15. FATF – Financial Action Task Force
16. SEC – Securities and Exchange Commission
17. AJF – Alert Justification Form
18. CSF – Client Suitability Form
19. I.C. – Insurance Commission

20. CITR – Covered Insurance Transaction Report
21. SITR – Suspicious Transaction Report
22. CRM – Customer Relation Management

B. **Anti-Money Laundering Council (AMLC)** - refers to the financial intelligence unit of the Philippines which is the government agency tasked to implement the AMLA and The Terrorism Financing Prevention and Suppression Act (TFPSA);

C. **Anti-Terrorism Council (ATC**) - refers to the Council created by virtue of Republic Act no. 9372, otherwise known as the "Human Security Act" (HSA) of 2007;

D. **Covered Person**, natural or juridical, refers to:

(1) Insurance companies, pre-need companies and all other persons supervised or regulated by the Insurance Commission (IC);
(2) Banks, non-banks, quasi-banks, trust entities, non-stock savings and loan associations, foreign exchange dealers, pawnshops, money changers, remittance and transfer companies, electronic money issuers and other financial institutions which under special laws supervised or regulated by the Bangko Sentral ng Pilipinas (BSP), including their subsidiaries and affiliates. For this purpose, a Subsidiary is an entity more than 50% of its outstanding voting stock is owned by a covered person, while an Affiliate is an entity, the voting stock of which at least 20% but not more than 50% is owned by a covered person;
(3) (i) securities dealers, brokers, salesmen, investment houses and other similar persons managing securities or rendering services as investment agent, advisor, or consultant, (ii) mutual funds, close-end investment companies, common trust funds, and other similar persons, and (iii) other entities administering or otherwise dealing in currency, commodities or financial derivatives based thereon, valuable objects, cash substitutes and other similar monetary instruments or property supervised or regulated by the Securities and Exchange Commission (SEC);
(4) Jewelry dealers in precious metals, who, as a business, trade in precious metals, for transactions in excess of One million pesos (P1,000,000.00);
(5) Jewelry dealers in precious stones, who, as a business, trade in precious stones, for transactions in excess of One million pesos (P1,000,000.00);
(6) Company service providers which, as a business, provide any of the following services to third parties: (i) acting as a formation agent of juridical persons; (ii) acting as (or arranging for another person to act as) a director or corporate secretary of a company, a partner of a partnership, or a similar position in relation to other juridical persons; (iii) providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; and (iv) acting as (or arranging for another person to act as) a nominee shareholder for another person; and
(7) Persons who provide any of the following services:

(i) managing of client money, securities or other assets;
(ii) management of bank, savings or securities accounts;
(iii) organization of contributions for the creation, operation or management of companies; and

(iv) creation, operation or management of juridical persons or arrangements, and buying and selling business entities.

Notwithstanding the foregoing, the term 'covered persons' shall exclude lawyers and accountants acting as independent legal professionals in relation to information concerning their clients or where disclosure of information would compromise client confidences or the attorney-client relationship: Provided, That these lawyers and accountants are authorized to practice in the Philippines and shall continue to be subject to the provisions of their respective codes of conduct and/or professional responsibility or any of its amendments.

E. **Money Laundering** – is committed by any person who, knowing that any monetary instrument or property represents, involves, or relates to the proceeds of any unlawful activity:

a. transacts said monetary instrument or property;
b. converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;
c. conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;
d. attempts or conspires to commit money laundering offenses referred to in paragraphs (a), (b) or (c) above;
e. aids, abets, assists in or counsels the commission of the money laundering offenses referred to in paragraphs (a), (b) or (c) above; and
f. performs or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in paragraphs (a), (b) or (c) above.

Money laundering is also committed by any covered person who, knowing that a covered or suspicious transaction is required under any of the AMLA provisions, as amended, its RIRR or under this Manual, to be reported to the Anti-Money Laundering Council (AMLC), fails to do so.

In a broader sense, it is the process of transferring the proceeds of criminal activities into the legitimate mainstream of commerce by concealing their origin. Anyone who conducts a financial transaction with knowledge that the funds are proceeds of an unlawful activity is generally considered to be laundering money.

STAGES OF ML

Generally, the process of Money Laundering comprises three stages which may be numerous transactions that could alert the Company to the money laundering activity:

(a) **Placement** – physical disposal of cash proceeds derived from illegal activity.

(b) **Layering –** separating illicit proceeds from their source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity or to obscure the source of the funds.

(c) **Integration** – the provision of apparent legitimacy to criminally-derived wealth. If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds.

F. **Financing of Terrorism** – a crime committed by a person who, directly or indirectly, willfully and without lawful excuse, possesses, provides, collects or uses property or funds or makes available property, funds or financial service or other related services, by any means, with the unlawful and willful intention that they should be used or with the knowledge that they are to be used in full or in part;
1) to carry out or facilitate the commission of any act of terrorism,
2) by a terrorist organization, association or group; or
3) by an individual terrorist.

G. **Dealing with regard to property or funds** - refers to receiving, acquiring, transacting, representing, concealing, disposing, converting, transferring or moving, using as security or providing financial services.

H. **Designated persons** - refer to:

1. Any person or entity designated as a terrorist, one who finances terrorism, or a terrorist organization or group under the applicable United Nations Security Council Resolution or by another jurisdiction or supra-national prescribed jurisdiction;
2. Any organization, association, or group of persons proscribed pursuant to Section 17 of the HSA of 2007; or
3. Any person, organization, association, or group of persons whose property or funds, based on probable cause are subject to seizure and sequestration under the existing law.

I. **"Designation" or "Listing"** - refers to the identification of a person, organization, association or group of persons that is subject to targeted financial sanctions pursuant to the applicable United Nations Security Council Resolutions.

J. **Forfeiture** - refers to a court order transferring in favor of the government, after due process, ownership of property or funds representing, involving, or relating to financing of terrorism as defined in Section 4 or an offense under Sections 5, 6, 7, 8, or 9 of the TF Suppression Act.

K. **Freeze** - refers to the blocking or restraining of specific property or funds from being transacted, converted, concealed, moved, or disposed of without affecting the ownership thereof.

L. "**Probable cause**" - refers to a reasonable ground of suspicion supported by circumstances warranting a cautious person to believe that property or funds are in any way related to terrorism financing, acts of terrorism or other violations under the TF Suppression Act.

M. **Terrorist** - refers to any natural person who: (a) commits, or attempts, or conspires to commit terrorist acts by any means, directly or indirectly, unlawfully, and willfully; (b) participates, as a principal, or as an accomplice, in terrorist acts; (c) organizes or directs

others to commit terrorist acts; or (d) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist acts or with the knowledge of the intention of the group to commit terrorist acts.

N. **Terrorist acts** - refer to the following:

1. Any act in violation of Section 3 or 4 of the HSA of 2007.
2. Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.
3. Any act which constitutes an offense that is within the scope of any of the following treaties to which the Republic of the Philippines is a State party:
   a. Convention for the Suppression of Unlawful Seizure of Aircraft, done at The Hague on 16 December 1970;
   b. Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971;
   c. Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents, adopted by the General Assembly of the United Nations on 14 December 1973;
   d. International Convention against the Taking of Hostages, adopted by the General Assembly of the United Nations on 17 December 1979;
   e. Convention on the Physical Protection of Nuclear Material, adopted at Vienna on 3 March 1980;
   f. Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 24 February 1988;
   g. Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, done at Rome on 10 March 1988;
   h. Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the Continental Shelf, done at Rome on 10 March 1988;
   i. International Convention for the Suppression of Terrorist Bombings, adopted by the General Assembly of the United Nations on 15 December 1997.

O. **Terrorist Organization, Association or Group of Persons** - refers to any entity owned or controlled by any terrorist or group of terrorists that: (1) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (2) participates as an accomplice in terrorist acts; (3) organizes or directs others to commit terrorist acts; or (4) contributes to the commission of terrorist acts by a group of persons acting with common purpose of furthering the terrorist acts where the contribution is made intentionally and with the aim of furthering the terrorist acts or with the knowledge of the intention of the group to commit terrorist acts.

P. **Monetary instrument** refers to:

a. Contracts or policies of insurance, life of non-life, and contracts of surety ship, pre – need plans and member certificates issued by mutual benefit association;
b. Credit instruments, including bank deposits, financial interest, royalties, commissions and other intangible property
c. Drafts, checks, and notes;
d. Stocks or shares, participation or interest in a corporation, or in a commercial enterprise or profit-making venture and evidenced by a certificate, contract, instrument, whether written or electronic in character including those enumerated in Section 3 of the Securities Regulation Code.
e. Participation or interest in any non – stock, non – profit corporation
f. Securities or negotiable instruments, bonds, commercial papers, deposit certificates, trust certificates, custodial receipts of deposit substitute instruments, trading orders, transaction tickets and confirmations of sale or investments and money market instruments;
g. Coins of currency of legal tender of the Philippines, or of any other country; and
h. Other similar instruments where title thereto passes to another by endorsement, assignment or delivery.

Q. **Transaction** refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between the parties thereto. It also includes any movement of funds by any means with a Covered Person.

R. **Covered transaction (CT)** is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of five hundred thousand pesos (P500, 000.00) within one banking day.

S. **Suspicious Transaction (ST)** under Circular 706 and RA 10167 are transactions with Covered Persons, regardless of the amount involved, where any of the following circumstances exist:

1. There is no underlying legal or trade obligation, purpose or economic justification;
2. The client is not properly identified;
3. The amount involved is not commensurate with the business or financial capacity of the client;
4. Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the Act.
5. Any circumstance relating to the transaction which is observed to deviate from the profile of the client and/or the client's past transactions with the Covered Person;
6. The transaction is in any way related to an unlawful activity or any money laundering activity or offense that is about to be, is being or has been committed;

7. Any transactions that is similar, identical or analogous to any of the foregoing.
8. Any unsuccessful attempt to transact with a covered person, the denial of which is based on any of the foregoing circumstances, shall likewise be considered as suspicious transaction.

Suspicious Transaction defined under RA 10168 – refers to a transaction with a Covered Person, regardless of the amount involved that is, in any way, related to terrorism financing or terrorist acts. It includes attempted transactions made by suspected or designated terrorist individuals, organizations, associations or groups of persons. In determining whether a transaction is suspicious, Covered Persons should consider the following circumstances:

1. Wire transfers between accounts, without visible legal, economic or business purpose, especially if the wire transfers are effected through countries which are identified or connected with terrorist activities;
2. Sources and/or beneficiaries of wire transfers are citizens of countries which are identified or connected with terrorist activities;
3. Repetitive deposits or withdrawals that cannot be satisfactorily explained or do not make economic or business sense;
4. Value of the transaction is grossly over and above what the client is capable of earning;
5. Client is conducting a transaction that is out of the ordinary for his known business interests;
6. Deposits by individuals who have no known connection or relation with the account holder;
7. Client is receiving remittances from a country where none of his family members is working or residing;
8. Client was reported and/or mentioned in the news to be involved in terrorist activities;
9. Client is under investigation by law enforcement agencies for possible involvement in terrorist activities;
10. Transactions of individuals, companies or Non-Government Organizations (NGOs)/Non-Profit Organizations (NPOs) that are affiliated or related to people suspected of having connection with a terrorist individual, organization, association or group of persons;
11. Transactions of individuals, companies or NGOs/NPOs that are suspected of being used to pay or receive funds from a terrorist individual, organization, association or group of persons;
12. The NGO/NPO does not appear to have expenses normally related to relief or humanitarian efforts;
13. The absence of contributions from donors located within the country of origin of the NGO/NPO;
14. The volume and frequency of transactions of the NGO/NPO are not commensurate with its stated purpose and activity.

T. **Unlawful Activity** refers to any wrongful act or omissions which are contrary to the law. This violation includes illegal activities, forbidden or disapproved deeds and immoral acts and against public policy that will constitutes a criminal act or series or combination thereof involving or having direct relation to the following:

1. Kidnapping for ransom under Article 267 of Act No. 3815, otherwise known as the Revised Penal Code, as amended;

2. Sections 4, 5, 6, 8, 9, 10, 12, 13, 14, 15, and 16 of Republic Act No. 9165, otherwise known as the Comprehensive Dangerous Drugs Act of 2002;
3. Section 3 paragraphs B, C, E, G, H, and I of Republic Act No. 3019, as amended; otherwise known as the Anti-Graft and Corrupt Practices Act;
4. Plunder under Republic Act No. 7080, as amended;
5. Robbery and extortion under Articles 294, 295, 296, 299, 300, 301, and 302 of the Revised Penal Code, as amended;
6. Jueteng and Masiao punished as illegal gambling under Presidential Decree No. 1602;
7. Piracy on the high seas under the Revised Penal Code, as amended and Presidential Decree No. 532;
8. Qualified theft under Article 310 of the Revised Penal Code, as amended;
9. Swindling under Article 315 and "Other Forms of Swindling" under Article 316 of the Revised Penal Code, as amended;
10. Smuggling under Republic Act Nos. 455 and 1937, as amended, of the Tariff and Customs Code of the Philippines;
11. Violations under Republic Act No. 8792, otherwise known as the Electronic Commerce Act of 2000;
12. Hijacking and other violations under Republic Act No. 6235; destructive arson and murder, as defined under the Revised Penal Code, as amended, including those perpetrated by terrorists against non-combatant persons and similar targets;
13. Terrorism and conspiracy to commit terrorism as defined and penalized under Sections 3 and 4 of Republic Act No. 9372;
14. Financing of terrorism under Section 4 and offenses punishable under Sections 5, 6, 7 and 8 of Republic Act No. 10168, otherwise known as the Terrorism Financing Prevention and Suppression Act of 2012
15. Bribery under Articles 210, 211 and 211-A of the Revised Penal Code, as amended, and Corruption of Public Officers under Article 212 of the Revised Penal Code, as amended;
16. Frauds and Illegal Exactions and Transactions under Articles 213, 214, 215 and 216 of the Revised Penal Code, as amended;
17. Malversation of Public Funds and Property under Articles 217 and 222 of the Revised Penal Code, as amended;
18. Forgeries and Counterfeiting under Articles 163, 166, 167, 168, 169 and 176 of the Revised Penal Code, as amended;
19. Violations of Sections 4 to 6 of Republic Act No. 9208, otherwise known as the Anti-Trafficking in Persons Act of 2003 as amended;
20. Violations of Sections 78 to 79 of Chapter IV, of Presidential Decree No. 705, otherwise known as the Revised Forestry Code of the Philippines, as amended;
21. Violations of Sections 86 to 106 of Chapter VI, of Republic Act No. 8550, otherwise known as the Philippine Fisheries Code of 1998;
22. Violations of Sections 101 to 107, and 110 of Republic Act No. 7942, otherwise known as the Philippine Mining Act of 1995;
23. Violations of Section 27(c), (e), (f), (g) and (i), of Republic Act No. 9147, otherwise known as the Wildlife Resources Conservation and Protection Act;
24. Violation of Section 7(b) of Republic Act No. 9072, otherwise known as the National Caves and Cave Resources Management Protection Act;
25. Violation of Republic Act No. 6539, otherwise known as the Anti-Carnapping Act of 2002, as amended;

26. Violations of Sections 1, 3 and 5 of Presidential Decree No. 1866, as amended, otherwise known as the Decree Codifying the Laws on Illegal/Unlawful Possession, Manufacture, Dealing in, Acquisition or Disposition of Firearms, Ammunition or Explosives;
27. Violation of Presidential Decree No. 1612, otherwise known as the Anti-Fencing Law;
28. Violation of Section 6 of Republic Act No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995, as amended by Republic Act No. 10022;
29. Violation of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines;
30. Violation of Section 4 of Republic Act No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009;
31. Violation of Section 4 of Republic Act No. 9775, otherwise known as the Anti-Child Pornography Act of 2009;
32. Violations of Sections 5, 7, 8, 9, 10(c), (d) and (e), 11, 12 and 14 of Republic Act No. 7610, otherwise known as the Special Protection of Children Against Abuse, Exploitation and Discrimination;
33. Fraudulent practices and other violations under Republic Act No. 8799, otherwise known as the Securities Regulation Code of 2000; and
34. Felonies or offenses of a similar nature to aforementioned unlawful activities that are punishable under the penal laws of other countries. In determining whether or not a felony or offense punishable under the penal laws of other countries is "of similar nature", as to constitute an unlawful activity under the AMLA, the nomenclature of said offense or felony need not be identical to any of the unlawful activities listed above.

U. **Proceeds** – refers to an amount derived or realized from any unlawful activity;

V. **Customer/Client –** refers to any person who keeps an account, or otherwise transacts business with an ICRE. It includes the following:

(1) Beneficial owner, or any natural person who ultimately owns or controls a customer and/or on whose behalf an account is maintained, or a transaction is conducted;
(2) Transactors, agents, and other authorized representatives of beneficial owners;
(3) Beneficiaries;
(4) A company or person whose assets are managed by an asset manager;
(5) Trustors/grantors/settlors of a trust; and,
(6) Insurance policy holder/owner, insured, pre-need plan holder, HMO client or HMO enrolled member, whether actual or prospective.

W. **Shell Company**- Legal entities which have no business substance in their own right but through which financial transactions may be conducted.

X. **Shell Bank**- a shell company incorporated as a bank or made to appear to be incorporated as a bank but has no physical presence and no affiliation with a regulated financial group. It can also be a bank that (1) does not conduct business at a fixed address in a jurisdiction in which the shell bank is authorized to engage; (2) does not employ one or more individuals on a full time basis at this fixed address; (3) does not maintain operating records at this address, and (4) is not subject to inspection by the authority that licensed it to conduct banking activities.

Y. **Beneficial Owner** – refers to any natural person who:

1. Ultimately owns or controls a customer and/or on whose behalf a transaction or activity is being conducted; or,
2. Has ultimate effective control over a legal person or legal arrangement; or,
3. Owns the same percentage as prescribed in the Guidelines or Identifying Beneficial Ownership and 2018 IRR and its succeeding future amendments.

Control includes whether the control is exerted be means of trusts, agreements, arrangements, understandings, or practices whether or not the individual can exercise control through making decisions about financial and operating policies.

Z. **Politically Exposed Person or PEP** – refers to an individual who is or has been entrusted with prominent public positions 1) in the Philippines with substantial authority over policy, operations or the use or allocation of government – owned resources; 2) a foreign state; or 3) an international organization.

The term shall likewise include immediate family members, and close relationships and associates that are reputedly known to have 1.1) joint beneficial ownership of a legal entity or legal arrangement with the main/principal PEP or 1.2) sole beneficial ownership of a legal entity or legal arrangement that is known to exist for the benefit of the main/principal PEP.

Immediate family members of PEPs refer to individuals related to the PEP within the second degree of consanguinity or affinity.

Spouse or partner, children and their spouses, and parents and parents – in – law.

Close relationships/associates of PEPs refers to persons who are widely and publicly known, socially or professionally. To maintain a particularly close relationship with the PEP, and include persons who are in the position to conduct substantial domestic and international financial transactions on behalf of the PEP.

Persons widely and publicly known to maintain a particularly close relationship with the PEP, and include persons who are in a position to conduct substantial domestic and international financial transactions on behalf of the PEP.

AA. **Correspondent banking** refers to the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank).

BB. **Fund/Wire Transfer** – refers to any transaction carried out on behalf of an originator (both natural and juridical) through a financial institution (Originating Institution) by electronic means with a view to making an amount of money available to a beneficiary at another financial institution (Beneficiary Institution). The originator person and the beneficiary person may be the same person.

CC. **Cross Border Transfers** – any wire transfer where the originating and beneficiary institutions are located in different countries. It shall also refer to any chain of wire transfers that has at least one cross-border element.

DD. **Domestic Transfer** – any wire transfer where the originating and beneficiary institutions are located in the same country. It shall refer to any chain of wire transfers that takes place entirely within the borders of a single country, even though the system used to effect the fund/wire transfer may be located in another country.

EE. **Originating Institution** – refers to the entity utilized by the originator to transfer funds to the beneficiary and can either be (a) a Covered Person as specifically defined by these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than Covered Persons referred to in (c) but conducts business operations and activities similar to them.

FF. **Beneficiary Institution** – refers to the entity that will pay out the money to the beneficiary and can either be (a) a Covered Person as specifically defined by these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than Covered Persons referred to in (a) but conducts business operations and activities similar to them.

GG. **Intermediary institution** – refers to the entity utilized by the originating and beneficiary institutions where both have no correspondent banking relationship with each other but have established relationship with the intermediary institution. It can be either be (a) a Covered Person as specifically defined by these Rules and as generally defined by the AMLA, as amended, and its RIRR, or (b) a financial institution operating outside the Philippines that is other than Covered Persons referred to in (a) but conducts business operations and activities similar to them.

HH. **Monetary instrument or property related to an unlawful activity -** refers to (1) All proceeds of an unlawful activity; (2) All monetary, financial or economic means, devices, accounts, documents, papers, items or things used in or having any relation to an unlawful activity;(3) All moneys, expenditures, payments, disbursements, costs, outlays, charges, accounts, refunds and other similar items for the financing operations, and maintenance of any unlawful activity; and (4) For purposes of freeze order and bank inquiry: related and materially linked accounts. "*Related accounts*" refer to those accounts, the funds and sources of which originated

from and/or are materially linked to the monetary instruments or properties subject of the freeze order or an order of inquiry;

Materially–linked Accounts shall include the following:

(1) All accounts or monetary instruments under the name of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or an order of inquiry;

(2) All accounts or monetary instruments held, owned, or controlled by the owner or holder of the accounts, monetary instruments, or properties subject of the freeze order or order of inquiry, whether such accounts are held, owned or controlled singly or jointly with another person;

(3) All "ln Trust For" accounts where either the trustee or the trustor pertains to a person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;

(4) All accounts held for the benefit or in the interest of the person whose accounts, monetary instruments, or properties are the subject of the freeze order or order of inquiry;

(5) All accounts of juridical persons or legal arrangements that are owned, or controlled or ultimately effectively controlled by the natural person whose accounts, monetary instruments or properties are subject of the freeze order or order of inquiry, or where the latter has the ultimate effective control; and,

(6) All other accounts, shares, units, or monetary instruments that are similar, analogous, or identical to any of the foregoing .

II. **Payable-through account** – a correspondent account that is used directly by third parties to transact business on their own behalf.

JJ. **Official document –** any of the following identification documents:

(1) For Filipino citizens: Those issued by any of the following official authorities:

a. Government of the Republic of the Philippines, including its political subdivisions, agencies, and instrumentalities;

b. Government-Owned or -Controlled Corporations (GOCCs); or

c. Covered persons registered with and supervised or regulated by the Bangko Sentral, SEC or I.C.;

(2) For foreign nationals: Passport or Alien Certificate of Registration

(3) For Filipino Students: School ID signed by the school Principal or Head of the educational institution, and

(4) For Low Risk Clients/Customers: any document or information reduced in writing which the Covered Person deems sufficient to establish the identity of the Client or Customer or Insured.

KK. Immediate Family Member of PEPs refers to individuals related to the PEP within the second degree of consanguinity or affinity.

LL. Close Relationships/Associates of PEPs refer to person who are widely and publicly

known, socially or professionally, to maintain a particular close relationships with the PEP, and include persons who are in the position to conduct substantial domestic and international financial transactions on behalf of the PEP.

Effects of money laundering:

- It can lead to inexplicable changes in money demand and increased prudential risks for the banking system (economic);
- It can lead to reduced foreign investments if a country's financial system is perceived to be subject to the control of organized crime (security);
- It can destabilize the economies as it infiltrates and corrupts financial, legal and even political institutions (political and economic); and
- It can seriously weaken the moral and ethical standards of society (social).

It is incumbent upon the insurance companies, banks and other financial institutions to avoid transactions that will assist criminals in laundering proceeds of their crime. Hence, Commonwealth Insurance Company and Agencies, Branch Offices, and Regional Offices support the international drive against serious crimes, especially drug trafficking and terrorism. The Company also supports the policy of the State to protect and preserve the integrity and confidentiality of bank accounts and to ensure that the Philippines shall not be used as a money-laundering site for the proceeds of any unlawful activity.

Commonwealth Insurance Company is updated in conformity with the State policy and consistent with the Revised Implementing Rules of R.A. No. 9160 (as amended) and the Anti-Money Laundering circulars issued by the Insurance Commission, the AMLC Revised Implementing Rules and Regulations of R.A. No. 9160 and the Bangko Sentral ng Pilipinas (Circular No. 950).

IV. BASIC PRINCIPLES AND POLICIES TO COUNTER-TERRORISM FINANCING:

A. Customer Acceptance Policy (Know your Customer (KYC))

Satisfactory evidence of the customer's and insured's identity shall be obtained. Moreover, effective procedures for verifying the bona fides of new customers shall be implemented. In this regard, the Board of Directors and Senior Management shall ensure that the Insurance Company is not used to facilitate money laundering. They shall direct all employees to exercise utmost diligence to ensure that adequate measures are implemented to prevent the Company from being unwittingly involved in such a criminal activity. As such, no new account shall be opened and created without full compliance with the requirement of KYC requirements.

B. Compliance with Laws and Regulations

Senior management shall ensure that insurance business is conducted in conformity with the highest ethical standards and those laws, rules and regulations issued by AMLA or its RIRR are strictly adhered to. Transactions shall not be allowed where there is good reason to believe that the client is engaged in money laundering activities.

CIC shall fully comply with these rules and existing laws aimed at combating money laundering and terrorist financing by making sure that officers and employees are aware of their respective responsibilities and carry them out in accordance with superior and principled culture of compliance.

C. Cooperation with Regulatory and Law Enforcement Agencies

The CIC shall fully cooperate with regulatory and law enforcement agencies within the legal constraints relating to customer confidentiality, particularly on matters relating to the Data Privacy Act. Appropriate measures (e.g., reporting to Anti-Money Laundering Council) shall be taken when there are reasonable grounds for suspecting money laundering.

D. Adoption of Policies and Procedures

Policies consistent with the principles set in the Anti-Money Laundering Law, Implementing Rules and Regulations and Operating Manuals issued by the I.C.and AMLC shall be adopted and properly disseminated. Specific control procedures for customer identification, record keeping and retention of transaction documents and reporting of covered and suspicious transactions shall be implemented.

Procedural aspects in compliance with KYC and CDD activities are hereby adopted by CIC in performing clients' identification and determining relevant information mainly in doing financial business.

CIC shall adopt and effectively implement a sound AML and terrorist financing risk management system that identifies, assesses, monitors and controls insurance risks associated with money laundering and terrorist financing.

E. CDD Standards

The ICRE shall implement the following standards of CDD.-

a. Identify and verify the identity of a customer using reliable, independent source documents, data or information;
b. Verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person;
c. Identify the beneficial owner and take reasonable measures to verify the identity of beneficial owner based on official documents, or using relevant information or data obtained from reliable sources, such that ICRE is satisfied that it knows who is the

F. Training on Anti-Money Laundering

All employees of CIC shall be provided with adequate training on anti-money laundering law, rules and regulations as well as the policies and procedures established by the Company to ensure awareness and compliance. Training on anti-money-laundering shall be on a regular basis to create awareness in new rules and regulations and to update on the latest trends and techniques applied by money launderers to make them more effective in preventing money laundering activities.

CIC shall conduct business in conformity with high ethical standards in order to protect its safety and soundness as well as the integrity of the insurance industry.

Towards this principle, all employees shall be provided with adequate training on anti-money laundering law, rules and regulations as well as the policies and procedures established by the company to ensure awareness and compliance. Training on AML/CFT shall be on regular basis to create awareness in new rules and regulations and to update on the latest trends and techniques applied by money launderers and terrorist financiers to make them more effective in preventing money laundering/terrorist financing activities.

Therefore, all employees are strictly mandated to lawfully abide with the MLTFPP of CIC in relation to issuances of AMLA or its IRR. Ensuring as such helps block laundered money from entering the business in whatever stage of money laundering it may use. Money transfers are strictly well monitored so that any potential avenue to transform illegal funds in whatever form may it be cash or online transaction to insurance policy accounts of CIC shall be prevented.

CHAPTER - 2
POLICIES, PROCEDURES AND CONTROLS

I. Insured/ Acceptance Policies:

1. It shall be the policy of the Company to require the **risk-based and tiered policy** for all clients regardless of whether they are small time clients or high net worth insured individuals;

2. The Company shall also require more extensive due diligence for high risk customers, such as those known in public as controversial personalities, those individuals holding high-profile public position and their associates or companies clearly related with them;

3. In all instances, the Company shall document how a specific customer/ insured was profiled (low, normal or high) and what standard of CDD (reduced average or enhanced) was applied;

4. Decisions to enter into insurance business relationships with high risk customers shall be taken exclusively at senior management level;

5. It shall be the policy of the Company not cover or insured those customers who refuse to produce the required identification papers and to discontinue insurance business relationship with customers, who after a series of follow up requests, failed to submit customer identification documents or company profile.

6. In designing a customer / insured acceptance policy, the following factors are considered:
   - Background and source of premiums;
   - Country of origin and residence or operations;
   - Public/high profile position of the insured or its directors/trustees, stockholders, officers and/or authorized signatory of the company
   - Linked accounts;
   - Watchlist of individuals and entities engaged in illegal activities or terrorist related activities as circularized by I.C., AMLC, and Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury and United Nations Sanctions List
   - Business activities; and
   - Type of services/products/transactions to be entered with the Covered Persons or entities.

II. Classification of Insured and Description:

The following are the classification of insureds and the corresponding description:

1. Low Risk

a. Insureds who are residents in the area where the office/branch is located;
b. Insured with regular employment;
c. Insured who are employed in the area where the office/branch is located;
d. Banking institutions, trust entities and quasi-banks authorized by the BSP to operate as such;
e. Publicly listed companies subject to regulatory disclosure requirements;
f. Government agencies including government owned and controlled corporations (GOCCs);
g. SEC-registered company;
h. Publicly-listed company subject to regulatory disclosure requirements by the SEC/PSE;
i. Partnership;
j. Association; and,
k. Company applying for TITF accounts

2. ***Normal Risk***

a. Individual insured or juridical person covered not falling under "Low Risk" or "High Risk"; and,
b. Individual or Authorized Signatory (in case of Corporation) who is a Rank and File PEP or PEPs who are no longer in office for the last 5 years or more.

3. ***High Risk***

a. Individual/Authorized Signatory (in case of Corporation) who is an **incumbent** Politically Exposed Persons (PEPs):
   i. Local Government Officials: Mayor, Governor, Congressman
   ii. National Government Officials: President, Vice-President and Senators
   iii. Judicial Officials: Justices (S.C./C.A/Ombudsman/C.T.A.), RTC Judges and/or Senior State Prosecutors
   iv. Uniformed Personnel: Police and Military Officials
   v. Appointive Government Officials: Cabinet Secretary and Undersecretary
   vi. Head of Government Owned or Controlled Corporations
   vii. Leaders of major National Political Parties
   viii. Heads of Foreign States

b. Individuals who present foreign-issued ID's;

c. Non-resident Foreigner;

d. Overseas Filipino Worker/Immigrant who is not able to provide valid Philippine-issued ID's;

e. Client's whose name is found in Watchlist Database as circularized by Insurance Commission, other domestic and international organizations such as, but not limited to, the NBI/FBI/Interpol, OFAC list, UN Sanctions List;

f. Cash-intensive businesses, i.e. Foreign Exchange Dealer, Money Changers or Remittance Agents;

g. Foundation;

h. US Indicia/Citizen;

i. Other High Risk Accounts:
   i. Dormant and/or Numbered Accounts;
   ii. Firm of lawyers or accountants - Account is under the name of Law Firm/Office and Accounting Firm/Office;
   iii. Trustee, Nominee, Agent or Intermediary account ;
   iv. Shell Company/ Shell Bank;
   v. Handling of "pooled" funds of entities such as mutual funds, money managers, trusts and foundations, and other professional intermediaries. The Company shall require the customer to disclose the identity/ies of the beneficial owner/s of the funds and those who are in

control of the funds invested. Any information gathered shall be verified from trustworthy parties such as banks, reputable law firms'/accounting firms or accessing public or private databases or official sources;

vi. Wire/Fund Transfers; and,

vii. High-risk customer - from a country that is recognized as having inadequate internationally accepted anti-money laundering standards under MLPP Chapter III, Section II.E.4.

III. Assessment:

1.) Insured Assessment Procedures

a. Prior to policy application, all new clients and/or applicants shall be subject to underwriting and risk assessment for purposes of determining insured classification and the due diligence on the insurance coverage required under the AML rules. CIC carefully evaluates each new client to ensure proper CDD procedures are applied.

b. The frontliner shall determine classification of risk using the insurance Assessment Form for its insured and the corresponding level of due diligence to be performed. The determination of level of CDD work that CIC employs at the time of account opening and on ongoing monitoring purposes is crucial for risk prevention.

c. Before accepting the risk, the Account Officer/Staff shall also check the name of the client against the watchlist database in the Compliance System. Any addition to the watchlist database (which the AMLC may issue from time to time) shall also be counter-checked against existing list of clients and/or insured checking with service other bureaus and agencies shall be performed for indication of questionable activities. The Account Officer/Staff or designated personnel shall print the report generated from the Compliance system and attach the same with the CAF; affixing his/her signature on the CAF manifesting that the required "Insure" / "Client Verification" process had been completed.

In Client Verification, covered persons are verified independently and the collected data or information during identification process is done in any and pursuant to the following alternatives:

a. Face to face contact;
b. Use of Information and Communication Technology (ICT);
c. By checking the genuineness of the proof of identity documents to the issuing office;
d. Such other methods of authentication based on reliable sources; and
e. Other relevant documents, data or information in supplemental to complete the verification procedure.

d. After determining the client classification, the Account Officer shall require client to submit information and identification documents according to the level of required customer due diligence.

2.) Risk Assessment. – The ICRE shall:

a. Take appropriate steps to identify, assess and understand its AML/CTF risks in relation to its customers, its business, products and services, geographical exposures, transactions, delivery channels, and size, among others; and appropriately define and document its risk based approach. The risk assessment shall include both quantitative and qualitative factors.
b. Institute the following processes in assessing their ML/TF risks:
   i.) Documenting risks assessments and findings;
   ii.) Considering all the relevant risks factors, including the results of national and sectoral risks assessments, before determining what is the level of overall risk and the appropriate level factors and type of mitigation to be applied;
   iii.) Keeping the assessment up-to-date through periodic review; and,
   iv.) Ensure submission of the risk assessment information as may be required by the IC.
c. Maintain AML/CTF prevention policies, procedures, processes and controls that are relevant and up-to-date in lien with the dynamic risk associated with its business, products and services and that of its customers.
d. Establish, implement, monitor and maintain satisfactory controls that are commensurate with the level of AML/CTF risk and take enhance measures on identified high risk areas, which should be incorporated in the ICRE's MTPP.
e. Conduct additional assessment as and when required by the IC; and,
f. Institutional risk assessment shall be conducted at least once every two (2) years, or as often as the Board or Senior Management bay direct, depending on the level of risk identified in the previous assessment, or other relevant AML/CTF developments that may have impact on the ICRE's operation.

IV. Customer Identification and Customer Due Diligence:

1. Customer Identification (Policies and Procedures)

A. Satisfactory evidence of the true and full identity, representative capacity, domicile, legal capacity, occupation or business purpose/s of the insured or clients, as well as other identifying information whether they be occasional or usual, shall be strictly obtained.

B. Face-to-Face contact – No new insured/clients application shall be accepted and created without face-to-face contact and personal interview between CIC duly authorized personnel and the potential customer, except as may be provided by existing rules and regulations of the Insurance Commission.

The use of Information and Communication Technology (ICT) in the conduct of face-to-face contact and interview is allowed provided that the designated CIC personnel/agent is in possession of and has verified the identification

documents submitted by the prospective client *prior* to the interview and the *entire procedure is documented*.

C. Insurance procured through a trustee, agent, nominee or intermediary

Where the insurance is procured through a trustee, agent, nominee or intermediary, CIC shall establish and record of the true and full identity and existence of both the (a) trustee, nominee, agent or intermediary and (b) trustor, principal, beneficial owner, or person on whose behalf the insurance policy is procured. CIC shall determine the true nature of the parties' capacities and duties by obtaining a copy of the written document evidencing their relationship and apply the same criteria for assessing the risk profile and determining the standard of due diligence to be applied to both.

In case of several trustors, principals, beneficial owners, or persons on whose behalf the policies are being procured, CIC, at the minimum, needs to obtain the true and full name, place and date of birth or date of registration, as the case may be, present address, nature of work or business, and source of premiums at the time the policy was procured and paid by them separately. Where CIC is required to report a CT or circumstances warrant the filing of an ST, it shall obtain such other information on every trustor, principal, beneficial owner, or person on whose behalf the insurance policy is being procured in order that a complete and accurate report may be filed with the AMLC.

In case the Company entertains doubts that the trustee, nominee, agent of intermediary is being used as a dummy in circumvention of existing laws, it shall apply enhanced due diligence or file a Suspicious Transaction Report, if warranted.

D. The Account officer/staff shall require the client or investor to accomplish **one (1) copy of Account Opening Folder** (Appendix A - Individual; Appendix B - Corporate). The client or investor shall complete the form in front of the Account Officer/staff/agent and provide the following minimum information including the specimen signature/s of the authorized signatory/ies and documents/proofs of legal existence:

CIC safeguards and adheres to risk based approached in addition to CDD and KYC in accepting clients' prior issuance or creation of his account. Variety of factors is considered such as background check, work or occupation or business, among others is assessed so those proper jurisdictions where the clients are based are accurately addressed.

Minimum Customer/Client Information and Identification Documents – The following are the minimum customer information and identification documents required in the conduct of CDD:

A.) For New Individual Customer/Client**.** The company/ICRE shall develop a systematic procedure for establishing the true and full identity of new individual customers/clients, and shall open and maintain the account relationship only in the true and full name of the account/relationship owner/s. Unless otherwise stated in this Guidelines, average customer due diligence requires that the ICRE shall gather from individual customers/clients, before or during the course of establishing business relationship, the following minimum identification information and valid identification document:

1. Identification Information:
   a. Full Name (such as maiden name, alias or nickname, etc.);
   b. Date of birth;
   c. Place of birth;
   d. Sex;
   e. Citizenship or nationality;
   f. Address;
   g. Contact Number or Information;
   h. Source of Fund
   i. Specimen signature or biometric information;
   j. Name, address, date and place of birth, contact number or information, sex, and citizenship or nationality of beneficiary and/or beneficial owner, whenever applicable.

2. Identification Documents;
   a. PhillD; or
   b. Other identification document, as herein defined.

B.) For New Customers/Clients that are Juridical Persons. The ICRE shall develop a systematic procedure for identifying customers/clients that are corporate, partnership and sole proprietorship entities, as well as their stockholders/partners/owners, directors, officers and authorized signatories. It shall open and maintain accounts only in the true and full name of the entity.

Prior to building business relations, CIC shall take reasonable steps in authenticating that the client is indeed an existent corporate or juridical entity which has not been or is not in the process of corporate dissolution, wound up, or in the process of being closed, shutdown, phased out or terminated

Unless otherwise stated in this Guidelines, average due diligence requires that ICRE shall obtain from their customers/clients that are juridical

persons the following minimum identification information and documents before or during the course of establishing business relationships:

1. Identification Information:
   a. Full name;
   b. Name of authorized representative/transactor/signer;
   c. Current office address;
   d. Contact number or information;
   e. Nature of business;
   f. Source of fund;
   g. Specimen signature or biometrics of the authorized representative/transact/signer; and,
   h. Name, address, date and place of birth, contact number or information, sex and citizenship or nationality of beneficiary and/or beneficial owner, if applicable.

2. Identification Documents:
   a. Certificates of Registration issued by the Department of Trade and Industry (DTI) for sole proprietors, or Certificate of Incorporation or Partnership issued by the Securities and Exchange Commission (SEC) for corporations and partnerships, respectively, and by the Bangko Sentral ng Pilipinas (BSP) for money changers/foreign exchange dealers and remittance agents, and by AMLC for covered persons;
   b. Articles of Incorporation/Partnership;
   c. Registration Data Sheet/Latest General Information Sheet;
   d. Secretary's Certificate citing the pertinent portion of the Board or Partner's Resolution authorizing the signatory to sign on behalf of the entity; and,
   e. For entities registered outside of the Philippines, similar documents and/or information duly authenticated be a senior officer of the covered person assigned in the country of registration; in the absence of said officer, the documents shall be authenticated by the Philippine Consulate, company register or notary public, where said entities are registered.

   The ICRE shall understand the nature of the customer's business, its ownership and control structure.

C.) Legal Arrangements (Trust or Other Similar Arrangements)

When performing customer due diligence in relation to customers that are legal arrangements, ICRE shall identify and verify the identity of the customer, and understand the nature of business, and its ownership and control structure.

Unless otherwise stated in this Guidelines, Average due diligence requires that ICRE shall obtain from the customers/clients that are legal arrangement the following minimum identification information and documents before or during the course of establishing business relationships:

1. Full name of legal arrangement;
2. Current office address and country of establishment;
3. Contact number or information, if any;
4. Nature, purpose and objects of legal arrangement;
5. The names of the settlor, the trustee, the trustor, the protector, if any, the beneficiary and any other natural person exercising ultimate effective control over the legal arrangement;
6. Deed of trust and other proof of existence; and,
7. Other requirements for juridical person, as applicable.

D.) Valid Identification Documents

Customers and the authorized signatory/ies of a corporate or juridical person who engage in a transaction with an ICRE for the first time shall be required to present the original and submit a clear copy of, at least, one (1) identification document.

In case the identification document does not bear any photo of the customer or authorized signatory, or the photo bearing ID or a copy thereof does not clearly show the face of the customer or authorized signatory, the IVRE may utilize ICT or any other technology to take the photo of the customer or authorized signatory.

E.) Identification and Verification of Agents

1. General Requirement. ICRE shall verify that any person purporting to act on behalf of a customer is so authorized, and identify and verify the identity of that person.

2. Where the account is opened or an occasional transaction in excess of threshold is conducted by any person in behalf of another, ICRE shall establish and record the true and full identity and existence of both the account holder or person purporting to act on behalf of the customer, and the beneficial owner or the principal on whose behalf the transaction is being conducted.

3. ICRE shall verify the validity of the authority of the agent. In case it entertains doubt as to whether the account holder or person purporting to act on behalf of the customer is being used as a dummy in circumvention of existing laws, it shall apply EDD and file an STR, if warranted.

F.) Verification of Beneficial Ownership

1. General Requirement. ICRE shall identify the beneficial owner and take reasonable measures to the identity of the beneficial owner, using relevant information or data obtained from a reliable sources, such that ICRE is satisfied that it knows who the beneficial owner is.

2. Document Evidencing Relationship. ICRE shall determine the true nature of the beneficial owner's capacities and duties vis-à-vis his agent by obtaining a copy of written document evidencing their relationship and apply the same standards for assessing the risk profile and determining the standard of CDD to be applied to both.

3. Timing of Beneficial Ownership Verification. ICRE shall verify the identity of the beneficial owner before or during the course of establishing a business or professional relationship, or conducting transactions for occasional customers in excess of the threshold. They may complete the BOV after the establishment of the business or professional relationship; Provided, that:
   a.) this occurs as soon as reasonably practicable;
   b.) this is essential not to interrupt the normal conduct of business; and,
   c.) the ML/TF risk are effectively managed.

G.) Verification of Beneficial Ownership for Juridical Persons.

For customers that are juridical person, the ICRE shall identify and take reasonable measures to verify the identity of beneficial owners through the following information:
a.) the identity of the natural persons, if any, who ultimately have controlling ownership interest in a juridical person;
b.) to the extent that there is doubt under item (a) above, as to whether the persons with the controlling ownership interest are the beneficial owners or where no natural person exerts control through ownership interests, the identity of the natural person, if any, exercising control over juridical person through any other means; and,
c.) where no natural person is identified stated above, the identity of the relevant natural persons who hold senior management positions.

H.) Verification of Beneficial Ownership for Legal Arrangement.

For customer that are legal arrangements, the ICRE shall identify and take reasonable measures to verify the identity of the beneficial owners through the following information:
a.) for trust, the identity of the trustors/grantors/settlors, the trustees, the beneficiaries or class of beneficiaries, the protector, if any, and

any other natural person exercising ultimate effective control over the trust agreement;

b.) for beneficiaries of trust agreements that are designated by characteristics or by class, sufficient information concerning the beneficiary to satisfy the covered person that it will be able to establish the identity of the beneficiary at the time of payout or when the beneficiary intends to exercise vested rights; and,

c.) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

In determining the reasonableness of the identity verification measures, ICRE shall consider the money laundering and terrorist financing risks posed by the customer and the business relationship.

I.) Compliance with the Guidelines on Identifying Beneficial Ownership. The ICRE shall comply with the responsibilities imposed under the AMLC's Guidelines on Identifying Beneficial Ownership and any amendments thereto.

E. Clients who engage in insurance transactions with Covered Persons for the first time shall be required to present the original and submit a clear copy of at least one (1) valid photo-bearing identification document issued by an official authority or of the government. Valid ID's include the following:

- Passport
- Driver's License
- PRC ID
- NBI Clearance
- Police Clearance
- Postal ID
- Voter's ID
- Barangay Certification
- Senior Citizen Card
- GSIS e-Card/UMID
- SSS Card
- TIN ID
- OWWA ID
- OFW ID
- Seaman's Book
- IBP ID
- Alien/Immigrant Certificate of Registration
- Government Office and GOCC ID
- DSWD Certification
- Philhealth Insurance Card ng Bayan
- Certification from the National Council for Welfare of Disabled Persons
- Company ID issued by private institutions supervised or regulated by either BSP, SEC or IC

- Student's ID
- SEC Certificate of Registration
- Business Registration Certificate
- Passports issued by foreign governments shall also be considered valid identification documents

F. Authentication of Specimen Signature and Identification Document (ID):

Photocopies of identification and legal documents shall always be authenticated or verified against the original documents to ensure validity and authenticity. However, certified true copies of the said documents shall be accepted in case the original documents are not available.

The Account Officer/Designated Marketing Officer or Agent who has face-to-face contact with and/or witnesses the signing of documents by the insured/client, shall authenticate the specimen signature on the provided space for this purpose in the Insured / Customer Data Sheet. The stamping of "Verified Against Original" on the photocopy of ID's presented shall be done and to be signed and dated by the attending CIC authorized personnel or agent.

G. Before establishing a business relationship with corporate clients/investors, a company search and/or other commercial inquiries shall be made to ensure that the prospective insured/client has not been, or is not in the process of being dissolved, struck off, wound-up or terminated. In case of doubt as to the identity of the company, its directors or the business, a search or inquiry with the Securities and Exchange Commission, SEC, DTI, and other government agencies shall be made.

H. For companies and businesses registered outside the Philippines, comparable documents duly authenticated by the Philippine Consulate where said companies are located shall be obtained.

I. The Senior Officer or a Designated Officer/Agent shall interview new insured applicant or those clients with non-recurring transactions with the Company.

J. Representatives, acting on behalf of a client or insured, shall be required to present a duly notarized authorization signed by the client or insured. In addition, identification documents (e.g., Employment/Company ID, Driver's License, Passport, SSS/GSIS ID) shall be obtained from the client's or insured's representative to ascertain his true identity.

K. For common insured/customers with banks, the Company shall rely on customer due diligence performed by the parent company. For this purpose, the designated officer of the bank shall accomplish the "Certification of KYC Reliance" which provides among others the following;(1) it has conducted the required customer identification procedures on the client/customer, inclusive of the face-to-face contact and custody of the mandated minimum information and documentary requirements and (2) it will provide to CIC, without delay, the relevant identification documents when so requested by the latter.

The Frontliner shall request for the Certification of KYC reliance from the originating bank or unit on the same date of the transaction and upon its receipt, the same shall be forwarded to the Operations Support Division. On a monthly basis, OSD shall review the completeness of KYC Reliance Certifications and make a follow-up, where necessary from the concerned bank branch or unit.

L. Business transactions shall not be conducted with prospective insured/clients who fail to provide evidence of their identity. This policy shall be properly disseminated to ensure public awareness. However, this will not preclude the Company from reporting suspicious transactions.

M. If during the business relationship, there is reason to doubt the accuracy of the information on the insured/client's identity, the following measures shall be taken to verify the identity of the insured/client or the beneficiary, whichever is applicable: (a) it shall be classified as high risk account subject to continuous monitoring and (b) disciplinary history and disclosure of past relevant sanctions shall be reviewed.

N. For large insured/clients, a prior bank/non-bank reference shall be requested. A letter inquiring about the client or insured shall be sent to the reference indicated.

O. When circumstances allow, a visual check of the business enterprise shall be performed to verify its actual existence and capability to provide the products or services indicated on the business documents and to accept the risk.

P. In case of doubt as to whether the trustee, nominee or agent is being used as dummy in circumvention of existing laws, further inquiries shall immediately be made to verify the status of the business relationship between the parties. If satisfactory evidence of the beneficial owners cannot be obtained, the Company shall apply the "Know Your Customer" principle in deciding whether or not to proceed with the business and accept the risk.

Q. Reasonable inquiries shall be made on accounts opened by a firm of lawyers or accountants when transactions passing through such accounts give cause for concern.

R. Corporate accounts shall be maintained only in the name of the account holder. Hence, the Company shall not open or keep anonymous, fictitious name, incorrect name and similar accounts.

S. Numbered Accounts/Fictitious Names. The Company shall maintain customer's account only in the true and full name of the account owner or insured. Anonymous accounts, accounts under fictitious names, numbered accounts and all other similar accounts shall be absolutely prohibited.

T. Foundations, Clubs and Associations – In addition to the identification documents required for Corporate Clients/Insured, the following incorporation papers/documents shall be obtained:

- Articles of Incorporation and By- Laws;
- Board Resolution or Secretary's Certificate to sign insurance policies;

- Board Resolution or Secretary's Certificate of Authorized Signatories Containing Specimen Signatures;
- Latest General Information Sheet showing the List of Names of Directors and Principal Stockholders;
- Sworn Statement as to Existence or Non-existence of Beneficial Owners;
- Description of the real purpose/activities of the client if the same is not expressly indicated in the Articles Incorporation and By-Laws;
- SEC registration certificate and/or SEC certification confirming legal existence of account holder.

The Company should verify information derived from the above-mentioned documents by at least one of the following, whichever is applicable:

- Obtaining an independent undertaking from a reputable and known firm of lawyers and accountants;
- Obtaining prior bank references;
- Accessing public and private databases or official sources.

After positively identifying the institution, steps should be taken also to identify and verify at least two (2) signatories and if they are not the key officers of the insured entity, the identity of the principal officers should be verified. For this purpose, the principals who should be identified are those persons exercising control or significant influence over the organization's assets. This includes members of a governing body, the President, any of the Board members, the Treasurer and all the signatories.

In all cases, independent verification should be obtained that the persons involved are true and authorized representatives of the institution. Independent confirmation should also be obtained for the purpose of the institution.

2. Customer Due Diligence

The Sales and Marketing Group and Operations Department shall comply with the following guidelines for establishing the true and full identity of the insured/customers:

A. Reduced Due Diligence for Low Risk Customer

i. For individual customers, CIC may open an account under the true and full name of the account owner/s upon presentation of acceptable identification card or official document as defined in this Manual or other reliable, independent source documents, data or information.

ii. For corporate, partnership, and sole proprietorship entities, and other entities such as banking institutions, trust entities and quasi-banks authorized by the BSP to operate as such, publicly listed companies subject to regulatory disclosure requirements, government agencies

including GOCCs, CIC may open an account under the official name of these entities with the minimum information/documents and Board Resolution duly certified by the Corporate Secretary authorizing the signatory to sign insurance applications data and policy on behalf on the entity, obtained at the time of account opening. Verification of the identity of the customer, beneficial owner or authorized signatory will be done after the establishment of the business relationship.

B. Average Due Diligence for Normal Risk Customers

For New Individual customers – CIC shall obtain at the time of account opening all the minimum information and confirming this information with the valid identification documents hereof from individual insured/customers before processing of insurance policy and/or establishing any business relationship.

New Corporate and Juridical Entity – CIC shall obtain the minimum information and/or documents and authorized signatory/ies of corporate and juridical entities before establishing business relationships.

C. Enhanced Due Diligence for High Risk customers

Whenever enhanced due diligence is applied as required by the customer identification policy, the Sales and Marketing Group shall, in addition to the minimum KYC identification requirements, shall do the following:

1.) Obtain additional information on insurable interest other than the minimum information and/or documents required for the conduct of average due diligence;

(a) In cases of individual insured, i. supporting information on the intended nature of the business relationship/source of premiums/source of wealth, ii. Reasons for the intended insurance application, iii. list of companies where he is a director, officer or stockholder, iv. list of insurance and banks where the individual has a policy or is maintaining an account, and v. other relevant information available through public databases or internet.

(b) For entities assessed as high risk customers, such as shell companies; i. prior or existing bank references, ii. the name, present address, nationality, date of birth, nature of work, contact number, and source of premium of each of the primary officers (President, Treasurer and authorized signatory/ies), stockholders owning at least 20% of the voting stock, and directors/trustees/partners as well as their respective identification documents; iii. volume of assets, other information available through public databases or internet; iv. supporting information on the intended nature of the business relationship, source of funds or source of wealth; and v. reasons for the intended or performed transactions.

2.) Conduct validation procedures on any or all of the information provided.

3.) Secure senior management approval or the AML Compliance Committee approval to commence business relationship.

4.) Conduct enhanced ongoing monitoring of the insurance coverage.

5.) Require the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Where additional information cannot be obtained, or any information or document provided is false or falsified, or the result of the validation process is unsatisfactory, CIC shall deny insurance application with the customer without prejudice to the reporting of a suspicious transaction to the AMLC when so warranted.

The Underwriting Department, on the other hand, in addition to profiling of customers and monitoring of their transactions, shall see to it that the requisites for the conduct of enhanced due diligence has been

complied with and the Sales and Marketing Group has obtained the abovementioned additional information and/or documents from its insured /clients and senior officer's approval.

Enhanced Due Diligence, Minimum Validation Procedures

In validating minimum EDD procedures, CIC shall include the assured, the beneficiary as well as co-signers in assessing relevant risk factor whether EDD is applicable. Whether EDD be minimum or high, CIC as a matter of standard and company procedure shall examine the background and purpose of all multifaceted unusually large transactions, all unusual patterns of transactions whether with economic effect or legal purpose, and other transactions that may be considered as doubtful. When identified with higher risk, CIC shall deem the client as high risk and a must to conduct a more thorough EDD client verification.

I. Individual Insured – Validation procedures include but are not limited to the following:

a) Confirming the date of birth from a duly authenticated official document;
b) Verifying the address through evaluation of utility bills, bank or credit card statement, sending thank you letters or other documents showing address or through on – site visitation;
c) Contacting the applicant/customer by phone or email;
d) Determining the authenticity of the identification documents through validation of its issuance by requesting a

certification from the issuing authority or by any other effective and reliable means;

e) Determining the veracity of the declared source of premium.

II. Corporate or Juridical Entities – Verification procedures shall include, but are not limited to the following:

a) Validating the source of premium from reliable documents such as audited financial statements, ITR, bank references, etc.
b) Inquiring from the supervising authority the status of the entity
c) Verifying the address through on-site visitation of the Company, sending thank you letters, or other documents showing address;
d) Contacting the entity by phone or email.

III. High Risk Customer – An insurance applicant/customer from a foreign jurisdiction that is recognized as having inadequate internationally accepted AML standards, or presents greater risk for ML/TF or its associated unlawful activities, shall be subject to ECDD. Information relative to these are available from publicly available information such as the websites of FATF, FATF Style Regional Bodies (FSRB) like the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities like the OFAC of the U.S. Department of the Treasury, or other reliable third parties such as regulators or exchanges, which shall be a component of the Company's customer identification process.

Whether higher risks are identified, covered persons shall inform the senior management before the disbursement of the policy proceeds, to conduct enhanced scrutiny on the total business relationship with the policyholder, and to deliberate filing a report in compliance with STR reporting guidelines.

IV. Shell Company/ Shell Bank – The Company shall undertake banking relationship with a shell company with extreme caution and always apply EDD on both the entity and its beneficial owner/s. Because of the dubious nature of shell banks, no shell bank shall be allowed to operate or be established in the Philippines. The Insurance Company shall refuse to enter into, or continue, correspondent banking relationship with them. It shall likewise guard against establishing insurance relations with foreign financial institutions that permit their accounts to be used by shell banks.

V. Prohibited Insurance Accounts – The Company shall maintain accounts only in the true and full name of the policy holder. The provisions of existing law to the contrary notwithstanding, anonymous accounts,

accounts under fictitious names, numbered checking accounts, and all other similar account shall be absolutely prohibited.

VI. Treatment of Dormant or Un-renewed Policy. Where an insured's policy considered dormant or un-renewed for a number of years and suddenly becomes unusually active again, it shall be carefully reviewed to ensure that the underwriting procedures and acceptance are followed.

CDD Standards - The ICRE shall implement the following standards of CDD.

a. Identify and verify the identity of customer using reliable, independent source documents, data or information;
b. Verify that any person purporting to act on behalf of the customer is so authorized , and identify and verify the identity of that person;
c. Identify the beneficial owner and take reasonable measure to verify the identity of the beneficial owner based on official documents, or using relevant information or data obtained from reliable sources, such that the ICRE is satisfied that it knows who is the beneficial owner. The ICRE should have a system to understand the nature of the customer's business and its ownership and control structure, in case of juridical persons or legal arrangements.
   The ICRE shall keep records of the actions taken in order to identify the beneficial owner;
d. Determine, understand and, as appropriate, obtain information on, the purpose and intended nature of the account, transaction, or business relationship with their customers; and,
e. Conduct ongoing diligence on the business relationship and scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with the ICRE's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

V. Customer Risk Profiling:

ICRE shall develop clear, and written graduated customer acceptance and identification policies and procedures, which shall include sanctions and screening.

It shall specify the criteria and description of the types of customers that are likely to pose low, normal, or high ML/TF risk to their operations, as well as the standards in applying simplified/reduced, average, and enhanced customer due diligence, including a set of conditions for the refusal to conduct transactions.

Enhanced Due Diligence shall be applied to customers that are assessed by the company/ICRE or under this Guidelines as high risk for ML/TF. For customers assessed to be low risk, the company/ICRE may apply simplified/reduced due diligence.

The ICRE shall develop a clear set of criteria for customer risk profiling and assessment. Criteria shall include, at least, three (3) of the following: Provided, that the ICRE is satisfied that customer's risk profile is sufficiently established: to wit-

a.) The customer risk (e.g. type of customer, occasional or one-off, legal person structure, PEP classification, included in the list);
b.) The nature of the service or product to be availed of by the customers;
c.) The delivery channels, including cash-based, face-to-face or non-face-to-face, or cross-border movement of cash;
d.) The purpose of the account or transaction;
e.) The amount of fund to be transacted by a customer or the size of the transactions undertaken or to be undertaken;
f.) The regularity or duration of the transaction;
g.) The fact that the customer came from high risk jurisdiction;
h.) The existence of suspicious transaction indicators;
i.) The source of fund and source of wealth;
j.) Nature of business and/or employment;
k.) Country of origin and residence of operations, or the fact that the customer came from a high-risk jurisdiction or geographical area;
l.) Watchlist of individuals and entities engaged in illegal activities or terrorist related activities as circularized by IC, BSP, AMLC, and other international entities or organization, such the Office of Foreign Asset Control (OFAC) or the U.S. Department of the Treasury and United Nations Sanctions List;
m.) Such other factors the company/ICRE may deem reasonable or necessary to consider in assessing the risk of the customer to ML and TF.

In assessing the risk profile of juridical persons, the covered person shall also consider the financial profile and other relevant information of the active authorized signatories.

The company/ICRE shall documents the risk profiling results, as well as how a customer was profiled and the standard of CDD being applied.

VI. Diligence Required:

In High-Risk Jurisdiction or Geographic Location. The company/ICRE shall apply enhanced due diligence, proportionate to the risk, to accounts, transactions, and business relationships with customers who are nationals or citizens from foreign jurisdiction or geographical location that presents greater risk for ML/TF or its associated unlawful activities, as recognized as having inadequate internationally accepted AML/CTF standards as determined by domestic or international bodies.
Information relative to this are available from publicly available information such as the websites of FATF, FATF Style Regional Bodies (FSRB) like the Asia Pacific Group on Money Laundering and the Egmont Group, national authorities like the OFAC of the U.S. Department of Treasury, or other reliable third parties such as

regulators of exchanges, which shall be competent of a ICRE's customer identification process.

The company/ICRE shall countermeasures (such as conduct of enhanced due diligence, limit business relationship or financial transaction with the identified country or persons in that country) proportionate to the risk when called upon to do so by the FATF, or independently of any call by the FATF to do so, when warranted.

Enhanced Due Diligence (EDD). The company/ICRE shall examine the background and purpose of all complex, unusually large transactions, all unusual patterns of transactions which have no apparent economic or lawful purpose, and other transactions that may be considered suspicious. Where the risks are higher, the ICRE shall conduct EDD.

The company/ICRE shall employ EDD if it acquire information that:

a.) Raises doubt as to the accuracy of any information or document provided by the customer or the ownership of the entity;
b.) Justifies re-classification of the customer from low or normal risk to high-risk;
c.) When establishing business relationship with any person from countries identified by the FATF or AMLC as having on-going or substantial ML/TF risks;
d.) Warrants the filing of a Suspicious Transaction Report (STR) exists, including information that:
    i. The customer is transacting without any purpose, economic justification, or underlying legal or trade obligation;
    ii. The customer is transacting an amount that is not commensurate to the business or financial capacity of the customer or deviates from the profile of that customer;
    iii. The customer might have structured transactions to avoid being the subject of a Covered Transaction Report;
    iv. The customer has been or is currently engaged in any unlawful activity;
    v. Raises suspicions that an intermediary is being used to circumvent anti-money laundering compliance measures.

Enhance Due Diligence Measures (EDDM). Whenever EDD is applied as required by this Guidelines, or by the ICRE's customer acceptance policy, or where the risk of ML/TF are higher, the company/ICRE shall perform the following:

a.) Gather information to support the following:
    i. Sources of wealth and fund;
    ii. Nature of occupation and/or business;
    iii. Reason for intended or performed transaction; and,
    iv. Other identification, which the company/ICRE deems necessary to verify the identity of the customer, and their agents and beneficial owners.

b.) Conduct additional validation procedures, such as:
    i. Verifying volume of assets, information available through public database, internet or other records;
    ii. Verifying the declared residence address and conducting face-to-face contact with the customers, their agents, and beneficial owners; and,
    iii. Other modes of validation, which the company/ICRE deems reliable.

c.) Secure the approval of senior management to commence or continue transacting with the customer;

d.) Conduct enhanced ongoing monitoring, including more frequent or regular updating of identification information and identification documents;

e.) Require the first payment to be carried out through an account in the customer's name with the bank subject to similar CDD standards, where applicable; and,

f.) Such other measure as the company/ICRE may deem reasonable or necessary.

Simplified or Reduced Due Diligence (SRDD). Where lower risks or ML/TF have been identified, through an adequate analysis of risk by the ICRE and based on the result of the institutional risk assessment, simplified or reduced customer due diligence measures may be applied, the simplified or reduce measures shall be commensurate with the lower risk factors. Examples of possible measures are:

a.) Verifying the identity of the customer and the beneficial owner after establishment of the business relationship;
b.) Reducing the frequency of customer identification updates;
c.) Reducing the degree of ongoing monitoring and scrutinizing transactions, based on a reasonable monetary threshold;
d.) Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified or Reduced Diligence Measures (SRDDM). These are not acceptable whenever there is suspicion of ML/TF, or where specific higher risk scenarios apply.

CDD For Life Insurance and Other Investment-Related Insurance Policies. The company/ICRE shall, in addition to the CDD measures required for the customer and the beneficial owner, conduct the following CDD measure on the beneficiaries of life insurance and other investment related insurance policies, as soon as the beneficiary/ies are identified/designated.

a.) For beneficiaries that are identified as specially named natural or legal persons or legal arrangements – by taking the name of the person.
b.) For beneficiaries that are designated by characteristics, by class or by other means – by obtaining sufficient information concerning the beneficiary to satisfy the ICRE that it will be able to establish the identity of the beneficiary at the time of payout (released of the proceeds).

Information collected under (a) and (b) above, should be recorded and maintained in accordance with the provisions under Title VI of this Guidelines.

For both cases above, the verification of the identity of the beneficiary should occur at the time of payout.

The company/ICRE should include the beneficiary of life insurance policy as a relevant risk factor in determining whether EDD measures are applicable. If the company/ICRE determines that the beneficiary who is a legal person or legal arrangement presents a higher risk, it shall take enhance measure which include reasonable measures to identify and verify the identity of the beneficial owner of the beneficiary, at the time of payout.

Company/ICRE shall take reasonable measures to determine whether the beneficiaries and/or, where required, the beneficial owner of the beneficiary, are PEPs. This should occur at the latest, at the time of payout. Where higher risk are identified, the entity/ICRE shall inform senior management before the payout of the policy proceeds, to conduct enhanced scrutiny on the whole business of the policy holder, and to consider making a suspicious transaction report.

Where an entity/ICRE is unable to comply with the foregoing, it should consider making a suspicious transaction report.

VII. Customer Verification, CDD Measures, and Tipping Off:

In general. The company/ICRE shall implement and maintain a system of verifying the true identity of their clients, including validating the truthfulness of the information and confirming the authenticity of the identification documents presented, submitted and provided by the customer, using reliable and independent sources, documents, data or information.

For customers that are juridical persons or legal arrangements, ICRE shall maintain a system of understanding the nature of the customer's business or profession, ownership and control structure, as well as the authority and identification of all persons purporting to act on their behalf. They shall verify the customer's identity through the following information:

a.) name, legal form and proof of existence;
b.) the powers and other legal requirements or contracts that regulate and bind the juridical person or legal arrangement, as well as the names of the relevant persons

having senior management position or perform significant responsibilities in the juridical person or legal arrangement; and,

c.) address of the registered office and, if different, the principal place of business.

The company/ICRE shall verify the identity of the customer before or during the course of establishing a business relationship, or conducting transactions for occasional customers. They may complete the verification process after the establishment of the business relationship, provided, that:

a.) Completion occurs as soon as reasonably practicable;
b.) Deferred customer verification process is essential so as not to interrupt the normal conduct of business; and,
c.) The ML/TF risks are effectively managed, taking into consideration risk and materiality.

The company/ICRE shall adopt risk management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.

The company/ICRE shall independently verify the collected identification information and document, through any of the following modes, unless otherwise provided in this Guidelines:

a.) Face-to-face contact;
b.) Use of Information and Communication Technology;
c.) By confirming the authenticity of the identification documents to the issuing office;
d.) Reliance on third parties and service providers; or,
e.) Such other methods of validation based on reliable and independent sources, documents, data, or information.

For Politically Exposed Person. The company/ICRE shall establish and record the true and full identities of PEPs, as well as their family members, close relationships/associates and entities related to them. It shall carefully consider a PEP's position and the positions' attendant risks with respect to money laundering and terrorist financing in determining what standard of due diligence shall apply to them.

A. In case of domestic PEPs or persons who have been entrusted with a prominent function by an International organization, in addition to performing the applicable diligence measure, the ICRE shall:
    1. Take reasonable measures to determine whether a customer, and his agent and beneficial owner are PEPs; and,
    2. In case when there is a higher risk business relationship, adopt the following measures:
        a.) obtain senior management approval before establishing or, for existing customers, continuing, such business relationships;
        b.) take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs; and,

c.) conduct enhanced ongoing monitoring on that relationship.

B. In relation to foreign PEPs, in addition to performing the applicable customer due diligence measures, the ICRE shall:

1. Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
2. Obtain senior management approval before establishing such business relationship;
3. Take reasonable measures to establish the source of wealth and source of funds of customers and beneficial owners identified as PEPs; and,
4. Conduct enhanced ongoing monitoring on that relationship.

Failure to Satisfactorily Complete CDD Measures. In case the company/ICRE is unable to comply with relevant CDD measures, it shall:

A. Refuse to open an account, commence business relations or perform the transaction; or shall terminate the business relationship; and,
B. File an STR in relation to the customer, if circumstances warrant.

CDD and Tipping Off. In cases where the company/ICRE form a suspicion of ML/TF and associated unlawful activities , and it reasonably believe that performing the CDD process will tip-off the customer, it need not pursue the CDD process, but should file an STR, closely monitor the account, and review the business relationship.

VIII. Employee Screening & Training:

The company shall further strengthen the implementation of strict recruitment policies in hiring its company employees especially its marketing staffs, insurance adjusters, agents and other related personnel. It also regularly conducts a mandatory trainings/seminars to continuously educate its marketing staffs and insurance agents for them to be updated on the current trends of the market.

Further, the company ensures that any of its officers, employees or agents that may be found to have committed, conspired, abetted or aided in the commission of anti-money laundering or financing terrorists shall be meted out by appropriate disciplinary measures, not to mention the criminal and civil actions which may be filed against them in court. Third persons who may also be found committing such violation against the company or its policyholders will be dealt in accordance with the law.

The Company shall provide basic non-life insurance education and training for all personnel, including officers and directors, to ensure that they are fully aware of their personal obligations and responsibilities in combating money laundering and be familiar with the system of reporting and investigating suspicious transactions.

The lecture/briefing on anti-money laundering shall generally be conducted by competent personnel of the Company. However, if necessary, the training functions can be assigned to outside party/ies provided due diligence is exercised to ensure that the person/s appointed is/are able to perform effectively.

The CIC Compliance Division shall formulate a non-life annual AML insurance training program aimed to provide efficient, adequate and continuous education program for all CIC personnel, including officers and directors, to ensure that they fully comply and are fully aware of their obligations and responsibilities in combating money laundering particularly in relation to insured identification process, record keeping requirements and CT/ST reporting and ample understanding of the internal reporting processes including the chain of command for the reporting and investigation of suspicious insurance and money laundering activities.

The timing and scope of training shall be based on the level of awareness and instruction needed for each group of employees:

a. ***For New Hires*** - a general appreciation of the background of money laundering and identification and reporting of suspicious transactions to the appropriate authority. This training shall be provided to all new employees regardless of seniority, which shall be conducted by CIC HRD within 30 days from effective date of hiring. This shall be conducted thru the use of AML Computer-Based Training (CBT) e-learning program followed by a written examination. An employee is considered to have passed the AML examination when he/she meets a passing rate of 75%. Those who fail the exam shall undertake to repeat the exam until he/she passes.

b. **A refresher training** shall be conducted, at least once a year, to remind key personnel of their responsibilities and to make them aware of any changes in insurance law, rules and regulations relating to money laundering as well as the internal policies and procedures.

The lecture/briefing on anti-money laundering and countering financing of terrorism shall be conducted by the Compliance Management Department officer/s. CMD may also invite external resource speaker/s to conduct workshop on AML/CFT. However, if necessary, the training functions can be assigned to outside party/ies provided due diligence is exercised to ensure that the person/s appointed is/are able to perform effectively.

The Compliance Officer/Coordinator shall regularly circulate compliance bulletins covering amendments in the anti-money laundering law and changes in the pertinent rules and regulations as well as Insurance Commission Circulars. Developments in the anti-money laundering campaign of the government shall also be advised to all concerned.

CIC's annual AML training program and records of all AML seminars and trainings conducted by CIC and / or attended by its personnel (internal or external), including copies of AML seminar / training materials, shall be appropriately kept by the Compliance and Administrative Division.

CHAPTER 3
IMPLEMENTATION and MONITORING (Ongoing & Manual)

I. IMPLEMENTATION OF A MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION PROGRAM (ML/TFPP):

A. The ICRE's Board of Directors (BOD) shall approve, and the compliance officer shall implement, a comprehensive risk-based MTPP geared towards the promotion of high ethical and professional standards and the prevention of ML and TF. The MTPP shall be in writing; consistent with the AML and CTF Laws, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuance; and its provision shall reflect the ICRE's corporate structure and risk profile. It shall be readily available in friendly user form, whether in hard or soft copy. Moreover, it shall be well disseminated to all officers and staff who are obligated, given their position to implement compliance measures. The ICRE shall design procedures that ensure an audit trail evidencing the dissemination of the MTPP to relevant officers and staff.

Where an ICRE operates at multiple location in the Philippines, it shall adopt an institution-wide MTPP to be implemented in a consolidated manner. Where an ICRE has branches, subsidiaries, affiliates or offices located within and/or outside the Philippines, there shall be a consolidated ML/TF risk management system to ensure the coordination and implementation of policies and procedure on a group-wide basis, taking into account local business considerations, the requirement of host jurisdiction and **the level of country risk**. Lastly, the MTPP shall be updated at least once every two (2) years or whenever necessary to reflect changes in AML/CTF obligations, ML and TF trends, detection techniques and typologies.

At a minimum, the MTPP's provisions shall include internal policies, controls and procedures on the following:

1. Risk assessment and management;
2. Detailed procedures of the ICRE's compliance and implementation of customer due diligence, record-keeping and transaction reporting requirements;
3. An effective and continuous AML/CTF training program for all directors, and responsible officers and employees, to enable them to fully comply with their obligations and responsibilities under AML and CTF Laws, their respective implementing rules and regulations, this Guidelines and other applicable IC and AMLC issuances, their own internal policies and procedures, and such other obligations as may be required by the IC and/or he AMLC;
4. An adequate risk-based screening and recruitment process to ensure that only qualified and competent personnel with no criminal record or integrity-related issues are employed or contacted by ICRE:
5. Independent audit function to test the system. The ICRE shall specify in writing the examination scope of independent audits, which shall include evaluation or examination of the following:
    a.) Risk assessment and management;
    b.) MTPP;

c.) Accuracy and completeness of customer identification information, covered and suspicious transaction reports, and all other records and internal controls pertaining to compliance with the AML and CTF Laws, their respective implementing rules and regulations, this Guidelines and other relevant IC and AMLC issuance;

6. A mechanism that ensures all deficiencies noted during inspection and/or regular or special compliance checking are immediately and timely corrected and acted upon;
7. Cooperation with the IC, AMLC and other competent authorities;
8. Designation of Compliance Officer at the management level, as the lead implementer of the ICRE's compliance program or creation of compliance unit;
9. The indication, assessment and mitigation of ML/TF risks that may arise from new business practices, services, technologies and products;
10. Adequate safeguards on the confidentiality and use of information exchange, including safeguard to prevent tipping off;
11. A mechanism to comply with free, inquiry and asset preservation orders and all directives of the AMLC; and,
12. A mechanism to comply with the provisions from conducting transactions with designated persons and entities, as set out relevant United Nations Security Council Resolutions (UNSCRs) relating to the preservation and suppression of terrorism and terrorist financing and financing of proliferation of weapons of mass destruction.

B. Financial groups are authorized to implement group-wide MTPP, which should be applicable, and appropriate to all branches and majority owned subsidiaries of the financial group. These shall include the measures set out above, and also:
   1. Policies and procedures for sharing information required for the purpose of CDD and risk management;
   2. The provision, at group-level compliance, audit, and/or AMLC/CTF functions, of customer, account, and transaction information from branches and subsidiaries when necessary for AML/CTF purposes. This should include information and analysis of transaction or activities which appear unusual if such analysis was done. Similarly branches and subsidiaries should receive such information from these group-level functions when relevant and appropriate to risk management; and,
   3. Adequate safeguards on the confidentiality and use of information exchanged, including safeguard to prevent **tipping off** . (is the process of letting the customer know that he is or might be the subject of suspicion; prejudicing an investigation).

C. Within one hundred eighty (180) days from the date of effectivity of this Guidelines, the company/ICRE shall prepare and have available for inspection their new/updated and BOD-approved MTPP embodying the principles and provisions stated therein.

   MTPP shall be regularly updated at least **once every two (2) years** to incorporate changes in AML policies and procedures, latest trends in ML and TF typologies, and latest pertinent IC and/or AMLC issuances. Any revision or update in the MTPP shall likewise be approved by the BOD.

   The Compliance Office shall submit to the IC **not later than fifteen (15) days** from the approval of the Board of Director of the new/updated MTPP, a sworn certification that new/updated MTPP has been prepared. Duly noted and approved by the ICRE's BOD.

IMPLEMENTATION: OF TARGETED FINANCIAL SANCTIONS

The company/ICRE shall secure the consent of all their customers to be bound obligations set out in the relevant United Nations Security Council Resolutions relating to the prevention and suppression of proliferation financing of weapons of mass destruction, including the freezing and unfreezing actions as well as prohibitions from conducting transactions with designate persons and entities.

II. ONGOING MONITORING:

A.) Company/ICRE shall, on the basis of materiality risk, conduct ongoing monitoring by establishing a system that will enable them to understand the normal and reasonable account or business activity of the customers and scrutinize transactions undertaken throughout the course of business relationship to ensure that the customer's accounts, including transactions being conducted, are consistent with the ICRE's knowledge of its customer, their business and risk profile, including the where necessary, the source of funds.

B.) ICRE shall apply EDD on the customer/client if it acquires information in the course of its customer account or transaction monitoring that:

1. Raises doubt as to the accuracy of any information or document provided or the ownership of the juridical person or legal arrangement;
2. Justifies reclassification of the customer from low or normal risk to higher risk pursuant to this Guidelines or by its own criteria;
3. Indicates that any of the circumstances for the filing of a suspicious transaction report exists such as but not limited to the following:
   a.) Transaction without any underlying legal or trade obligation, purpose or economic justification;
   b.) Transacting an amount that is not commensurate with the business or financial capacity of the customer or deviates from his profile;
   c.) Structuring of transaction in order to avoid being the subject of covered transaction reporting; or,
   d.) Knowing that the customer was or is engaged or engaging in any unlawful activity as herein defined.

C.) The company/ICRE shall, on the basis of materiality risk, ensure that the pertinent identification information and documents collected under the CDD process are kept up-to-date and relevant, by undertaking of reviews of existing records, particularly for higher risk categories customers. Updating of records shall be mandatory when enhanced ongoing monitoring process is warranted. The company shall document the actions taken in connection with updating of customer's record/information, and accordingly update customer's risk profile.

III. MANUAL MONITORING:

Companies/ICREs that are not required under this Guidelines to have an electronic system of flagging and monitoring transaction shall ensure that they have the means of flagging and monitoring the transactions. The monitoring system should be capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risks, and to regularly apprise the board of directors and senior management on AML/CTF. They shall maintain a register of all STs that have been brought to the attention of senior management whether or not the same was reported to the AMLC.

CHAPTER 4
RECORDS KEEPING MANAGEMENT, RETENTION and REQUIREMENTS

A. Record Keeping:

CIC shall comply with the guidelines on digitization of customer records (DIGICUR) and implements the digitization of all customer records and storing of such digitized records of clients in the central data base.

The covered person/company/ICRE shall maintain and safely store for five (5) years from the dates of transactions all customer records and transaction documents.

For Closed Accounts and Terminated Relationships - The company/ICRE shall keep all records obtained through CDD, account files and business correspondence, and result of any analysis undertaken, for at least five (5) years following the closure of account, termination of business or professional relationship or after the date of occasional transaction.

Retention of Records Where There is a Case - If a case has been filed in court involving the account, records must be retained and safely kept beyond the five (5) year period, until it is officially confirmed by the AMLC Secretariat that the case has been resolved, decided, or terminated with finality.

B. Safekeeping of Insurance Policies and Documents: CIC shall designate at least two (2) Officers who will be jointly responsible and accountable in the safekeeping of all insurance policies and documents required to be retained by the AMLA, as amended, its RIRR and this Manual. They shall have the obligation to make these policies and attached documents readily available without delay during SEC/AMLC regular or special examinations.

1. The Marketing Support Division Head shall be responsible and accountable for safekeeping of insurance policies and documents pertaining to insurance application, signature of policy holders and transaction trails.

2. Records of Covered and Suspicious Transaction reporting shall be maintained and safe kept by the Compliance and Administrative Division. A register of all reports made to the AMLC, as well as reports made by the directors, officers or employees relative to suspicious transactions, whether or not such were reported to the Council, shall be maintained. Said register shall contain details of the date on which the report is made, the person who makes the report and information sufficient to identify the relevant papers. In addition, the Compliance Division shall ensure that the reports and other records on all transactions brought to the attention of the AML/CFT Committee including those transactions that are not reported to the AMLC are complete and properly kept.

3. With respect to closed accounts, records on client identification, account files and business correspondence, must be preserved and safely stored for at least five (5) years from the dates when they were closed or deemed closed upon endorsement of concerned department that such is definitely closed account. CIC's record safekeeping procedure shall comply with the AMLA requirements as well as security measures ensures utmost confidentiality of such records and files. In addition, records are retained as originals (hardcopy) or photocopies (hard or soft copy) in such forms that is admissible in court pursuant to existing laws and rules promulgated by the Supreme Court.

C. Forms of Record: Complimented by the requirements under the Guidelines on Digitization of Customer Records, the company/ICRE shall retain all transaction records either in:

a.) Their original forms; or,

b.) Such other forms sufficient to permit reconstruction of individual transactions so as to provide admissible evidence in court.

The company shall keep electronic copies of all CTRs and STRs, for at least five (5) years, from the date of submission to the AMLC.

For low risk customers, the company/ICRE shall maintain and store, in whatever form, a record of information data and transaction sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity.

D. Availability of Records: The company/ICRE shall ensure that all CDD information and transaction records are available swiftly to domestic competent authorities in the exercise of their official functions or upon order by competent authority.

Company/ICRE shall take measures to ensure that customer records are submitted in the manner, quality and period that would assist the AMLC in its prompt financial investigations and institution of legal actions. For this purpose, the entity shall implement the guidelines on the digitization of customer records issued by the AMLC.

CHAPTER 5
DETECTION, INVESTIGATION, and REPORTING OF SUSPICIOUS TRANSACTIONS

A. Covered Transactions as defined under Section 3, paragraph (b) of R. A. No. 9160 (as amended) and Section 1 of R.A. No. 9194, is a transaction in cash or other equivalent monetary instrument involving a total amount in excess of Five Hundred Thousand Pesos (Php 500,000.00) within one (1) banking day.

B. Suspicious Transactions as defined under Section 3, paragraph (b-1) of R. A. No. 9160 (as amended) and Section 2 of R.A. No. 9194, are transactions with Covered Persons, regardless of the amounts involved, where any of the following circumstances exist:

a. There is no underlying legal or trade obligation, purpose or economic justification;

b. The client is not properly identified;

c. The amount involved or premium payment is not commensurate with the business or financial capacity of the insured or client;

d. Taking into account all known circumstances, it may be perceived that the client's transaction is structured in order to avoid being the subject of reporting requirements under the Act.

e. Any circumstance relating to the procurement of the policy which is observed to deviate from the profile of the client and/or the client's past transactions with the Covered Person;

f. The transaction is in any way related to an unlawful activity or offense under this Act that is about to be, is being or has been committed; or

g. Any transactions that is similar or analogous to any of the foregoing.

C. The Company officers and staff shall at all times be alert of any customers falling under the above circumstances.

D. Initial inquiries and, when necessary, further investigations on the source of premiums shall be immediately performed if any suspicious transaction is identified.

E. If the Operations Officer/Underwriter identifies a substantial increase in cash deposits or placements from an individual or local business entity, he/she shall satisfy himself/herself that the insured has a legitimate explanation for the unusual activity.

F. Investigation of Suspicious Transactions:

Any indication of suspicious procurement of insurance policy or activity shall be investigated to prevent money laundering and other illegal transactions of similar nature:

1. Any transaction that is outside the usual activity of a known insured/client or involving large sums of money in cash or financial instruments received from or payable to non-clients is potentially suspicious and shall be carefully examined.

2. The degree of investigation shall depend on what the Company knows about the client and the nature of the proposed transaction:

   a. The Company shall satisfy itself that the transaction is legitimate.

   b. A general explanation for an isolated transaction from highly regarded clients whose normal activity is known shall be obtained.
   c. A more detailed explanation for large transaction from clients shall be obtained. If the explanation is unsatisfactory, more information shall be obtained before a transaction is authorized or declined.
   d. The transaction shall be referred to higher authority or the AMLC Committee for disposition when in doubt.

3. If the Company's concerns are not resolved during discussion with the client, discreet inquiries shall be performed without his/her knowledge. Uncorroborated explanation from the insured/client shall not be relied on if the transaction is unusual or the potential for abuse is great. If necessary, independent verification for at least a material part of the explanation shall be obtained. The Company shall be alert that something may be wrong if minimal information provided by the client could not be verified independently.

4. The Insurance Company shall be vigilant for any unusual, strange and/or peculiar transactions. It shall always follow sound insurance practices.

The Operations Officer/Underwriter shall be particularly vigilant about unusual placement activity if its client is a foreign exchange, securities, commodity or precious metals dealer or is engaged in any other business, which is particularly susceptible to money laundering:

a. These customers shall be closely monitored.

b. The Company shall ensure that its file contains an explanation of unusual transactions.

c. Large/unusual transactions shall be reviewed with the Division or Group Head for advice, counsel and direction.

5. Follow-up calls or letter to the client's residence and/or place of business shall be made, thanking him/her for opening an account. Disconnected phone service warrants further investigation.

6. The concerned Officer/Staff who identified a suspicious transaction shall refer the suspected account to the Division Head for further verification.

G. Unusual and Suspicious Insurance Monitoring:

1. Monitoring System for Money Laundering – CIC shall ensure that it has the means of flagging and monitoring the insurance transactions below:

a. Covered and suspicious transaction monitoring – performs statistical analysis, profiling and able to detect unusual patterns of insurance account activity;

b. Watch list monitoring – checks the existing insured and database for any listed undesirable individual or corporation;

c. Investigation – checks for given names throughout the history of payment stored in the system;

d. Can generate all the CTRs of the Covered Person accurately and completely with all the mandatory field properly filled up;

e. Must provide a complete underwriting audit trail;

f. Capable of aggregating activities of a customer with multiple accounts on consolidated basis for monitoring and reporting purposes; and

g. Has the capability to record all STs and support the investigation of alerts generated by the system and brought to the attention of Senior Management whether or not a report was filed with the AMLC.

H. Reporting of Covered and Suspicious Transactions:

1. In general, the company /ICRE shall file all CTRs and STRs, in accordance with the registration and reporting guidelines of AMLC.

2. Should the transaction be determined to be both a covered (CT) and suspicious transaction (ST), the same shall be reported as a suspicious transaction (ST). In this regard, it shall be reported first as CTR, subject to updating if it is finally confirmed to be reportable as STR.

3. CTRs shall be filed within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from occurrence thereof.

4. When the total amount of the premium/fees for a policy, plan or agreement for the entire year, regardless of frequency of payment, exceeds Five Hundred Thousand Pesos (P500,000.00), such amount shall be reported as a covered transaction, even if the amount of amortizations are less than the threshold amount. The CTR shall be filed upon payment of the first premium/fee amount, regardless of the frequency of payments. Under this Rule, the ICRE shall file the STR only once every year until the policy, plan, or agreement matures or rescinded, whichever comes first.

5. CTR and STR shall be filed in the forms prescribed by the AMLC and shall be submitted in a secured manner in electronic form in conformity with the AMLC Reporting Procedure version.

6. No administrative, criminal or civil proceedings shall prosper against any person for having made a CTR or STR in the regular performance of duties and in good faith, whether or not such reporting results in any criminal prosecution under the AMLA or any other law of the Philippines.

7. Deferred Reporting of Certain Covered Transactions – Pursuant to AMLC Resolution No.58 dated 25 March 2005 as amended by AMLC Resolution No. 24 dated 18 March 2009, the following are considered as "non-cash, no/low risk covered transactions" the reporting of which to the AMLC are deferred:

    a. Transactions between banks and the BSP;
    b. Transactions between banks operating in the Philippines;
    c. Internal operating expenses of banks;
    d. Transactions involving transfer of funds from one deposit account to another deposit account of the same person within the same bank;
    e. Roll-overs of placements of time deposit; and
    f. Loan/Interest principal payment debited against borrower's deposit account maintained with the lending bank.

I. Suspicious Transaction Reporting Procedures:

Upon identification of unusual or suspicious procurement of insurance policies, the following procedures shall be followed:

1. The concerned department or business unit front liner or Operations personnel who identified a suspicious insurance transaction shall refer the suspected account to the Underwriter, Division Head or Group Head for further verification.

2. The Underwriter Division Head or Group Head shall evaluate the report and he/she is of the opinion that there is/are reasonable basis for the suspicion, shall prepare his/her evaluation report and shall be forwarded to the Compliance Officer/Coordinator.

3. Upon receipt of the reports, the Compliance Officer/Coordinator shall convene a meeting of the AML Compliance Committee to evaluate the reports and determine if the suspicion is based on reasonable grounds.

4. If the Committee decides that there is reasonable basis for considering a suspicious insurance transaction or other illegal activity, a Suspicious Insurance Transaction Report (SITR) must be sent to AMLC using the prescribed form duly signed by the Compliance Officer together with other supporting documents. The SITR shall be submitted to the AMLC immediately but not more than ten (10) calendar days from the date that the insurance transaction was determined to be suspicious.

5. In the event that urgent disclosure is required, particularly when the insurance coverage is part of an ongoing investigation, the Compliance Officer/Coordinator shall notify in writing the AMLC Committee.

6. The Company and its directors, officers and employees shall not warn the clients when information relating to them is being reported or will be reported to the AMLC or that a suspicious insurance transaction has been or is about to be reported, the contents of the report or any other information in relation to the insurable interest. Any information about such reporting shall not be published or aired, in any manner or form, by the mass media or through electronic mail or other similar devices. In case of violation, the concerned Officer or employee shall be held criminally liable.

7. A director, officer or employee of the Company who knows that the insured/client has engaged in any of the predicate crimes under R.A. No. 9160 (as amended) shall promptly report the matter to the Compliance Officer. In this regard, the Compliance Officer shall immediately report the details to the AML Compliance Committee and the AMLC.

8. If there are reasonable grounds to suspect that the insured/client has engaged in an unlawful activity, the AML Compliance Committee, on receiving such a report, shall promptly evaluate whether the suspicion if valid. The case shall be immediately reported to the AMLC unless the committee considers that such reasonable grounds do not exist. However, unreported suspicion shall be properly recorded.

9. A register of all reports made to the AMLC, as well as reports made by the directors, officers or employees relative to suspicious insurance procurement transactions, whether or not such were reported to the Council, shall be maintained. Said register shall contain details of the date on which the report is made, the person who makes the report and information sufficient to identify the relevant papers. In addition, the AMLC Committee shall ensure that the reports and other records on all insurance transactions brought to their attention, including transactions that are not reported to the AMLC are complete and properly kept.

CHAPTER 6:
RISK MANAGEMENT

CIC shall develop sound non-life insurance risk management policies and practices to ensure that risks associated with money-laundering such as counterparty, reputational, operational, and compliance risks are identified, assessed, monitored, mitigated and controlled, as well as to ensure effective implementation of these regulations, to the end that CIC shall not be used as a vehicle to legitimize proceeds of unlawful insurance activity or to facilitate of finance terrorism.

Four (4) Areas of Sound Risk Management Practices:

A. Active Board and Senior Management Oversight:

1. Board and Senior Management Oversight

   It shall be the ultimate responsibility of the Board of Directors to fully comply with the provisions of these rules, the AMLA, as amended and its RIRR. It shall ensure that oversight on the institution's compliance management is adequate.

   Senior Management shall oversee the day to day management of the covered person, ensure effective implementation of the AMLCFT policies approved by the Board and alignment of activities with the strategic objectives, risk profile and corporate values set by the BOD. Further, Senior Management shall establish a management structure that promotes accountability and transparency and upholds checks and balances.

2. Committee on Money Laundering

The Company shall set up a Committee on Money Laundering composed of the members of the Senior Management and the Compliance Officer. It shall be the designated unit responsible for advising management and staff on the issuance and implementation of policies, procedures and controls to promote adherence to R.A. No. 9160 (as amended), IRR and operating manuals and regulations issued by SEC and BSP. The internal guidelines shall include personnel training, reporting of covered and suspicious transactions, and generally, all matters relating to the prevention of money laundering.

3. Compliance Office and Designation of Compliance Officer

Management of the implementation of CIC's Money Laundering and Terrorist Financing Prevention Program (MLPP) shall be a primary task of the Compliance and Administrative Division and the designated Compliance Officer/Coordinator. To ensure independence of the division, it shall have a direct reporting line to the Board of Directors through the AMLC Committee on all matters related to AML and Terrorist Financing compliance and their insurance risk management.

The designated Compliance Officer, as duly approved by the Board of Directors to oversee and coordinate the implementation of the Compliance System, shall also oversee and coordinate the implementation of the Anti-Money Laundering Manual.

The following are the primary duties and responsibilities of the Compliance Officer in relation to anti-money laundering:

1. Responds sufficiently well to inquiries pertaining to the insurance and covered person and the conduct of its business;

2. Establishes and maintains a manual of compliance procedures in relation to the business of the Company;

3. Ensures compliance by the officers and employees with the provisions of the anti-money laundering law as amended, implementing rules and regulations and this Manual; conduct periodic compliance checking which covers, among others, evaluation of existing processes, policies and procedures including on-going monitoring of performance by staff and officers involved in ML and TF prevention, reporting channels, effectiveness of the electronic money laundering transaction monitoring system through sample testing and review of audit or examination reports. Further, to report to the AMLCC any compliance findings;

4. Ensures that infractions, discovered either by internally initiated audits, or by special or regular examinations conducted by applicable regulators are immediately corrected;

5. Apprises all responsible Officers and employees of all resolutions, insurance circulars and other issuances by the AMLC in relation to matters aimed at preventing MF and TF and organizes the timing of AML training of Officers and employees including refresher trainings;

6. Alerts senior management, the BOD or CIC AMLC Committee if it believes that the covered person is failing to appropriately address AML/CFT issues;

7 Acts as the liaison between the Company and the AMLC in matters relating to compliance with the provisions of the anti-money laundering law, rules and regulations; and

8 Prepares and submits to the AMLC written reports on the Company's compliance with the provisions of anti-money laundering law, rules and regulations, in such form and submitted at such time as the Council may determine.

B. Acceptable Policies and Procedures Embodied in a Money Laundering and Terrorist Financing Prevention Program (ML/TFPP):

CIC shall adopt a comprehensive and risk-based ML/TFPP geared toward the promotion of high ethical and professional standards and the prevention of the Company being used, intentionally or unintentionally, for money laundering and terrorism financing. The ML/TFPP shall be consistent with the AMLA, as amended, and the provisions set out in AMLC's 2016 RIRR of R.A. No. 9160.

It shall be in writing, approved by the Board of Directors, and well disseminated to all officers and staff who are obligated by law and by their program to implement the same.

C. Appropriate Monitoring and Management Information System:

CIC shall adopt an AML and terrorist financing monitoring system that is appropriate for their risk-profile and business complexity and in accordance with existing rules and regulations on AMLA under AMLC, SEC and the Insurance Commission. The system should be capable of generating timely, accurate and complete reports to lessen the likelihood of any reputational and compliance risks, and to regularly apprise the Board of Directors and Senior Management on anti-money laundering and terrorist financing compliance at least once every year or annually**.**

Manual monitoring – CIC need not have an electronic system but must ensure that it has the means of complying with the AML regulations, its internal policies and Compliance System Manual (Monitoring and Reporting Tools).

D. Periodic Audit:

The Internal Audit group of CIC shall perform a periodic review of the implementation of the policies and procedures indicated on the Anti-Money Laundering Manual to determine compliance with existing laws and regulations, evaluate adequacy and measure effectiveness. Any adverse findings shall be advised to the Compliance Officer or Compliance Coordinator and the AMLCC for appropriate action.

CHAPTER 7

CONTINUING EDUCATION and TRAINING PROGRAM

The Company/ICRE shall develop, or create opportunities for, continuing training and education program for its responsible directors, officers and employees to promote AML/CTF awareness and strong compliance culture.

The education and training shall include relevant topics, such as:

a. Overview on ML/TFP, and the AMLA;
b. Roles of Directors, officers and employees in ML/TFP prevention;
c. Risk management;
d. Preventive measures;
e. Compliance with freeze, bank inquiry and asset preservation orders, and all directives of the AMLC;
f. Cooperation with the AMLC and the IC; and,
g. International standards and best practices.

Attendance by company's/ICRE's directors, officers and employees in all education and training programs whether internally or externally organized, shall be documented. Copies of AML/CTF continuing education and training programs, training certificates, attendance and materials shall be made available to the IC and the AMLC upon request.

The company/ICRE shall provide refresher programs, at least every three (3) years. In cases where there are new developments brought about by new legislations, rules and regulations, and other IC and/or AMLC issuances, the company/ICRE shall immediately cascade these information to its responsible directors, officers and employees; Provided, that the cascading of the information is documented.[1]

[1] *(Itallics supplied)Pursuant to Sec. 29, of Circular Letter No. 2019-65 Of the Insurance Commission dated 22 November 2019.*

NOTE: Updated as of September 14, 2022 in compliance to AMLC Regulatory Issuance (ARI) A, B, and C, No. 2 s. 2018 and AMLC Regulatory Issuance (ARI) No. 6 s. 2021

BOARD APPROVAL:

RAFAEL C. REGALA
Chairman

MARIO A. NOCHE
Vice Chairman

LOURDES M. CORCELLES
Corporate Secretary

JOSE PAOLO F. NOCHE
Director

REMIE G. TIMBREZA
Director

JUAN T. TAJANLANGIT, JR.
Director

EDGARDO P. IDQUIVAL
Director

LUCITA P. PANTIG
Director

ELVIRA E. LASCANO
Independent Director

RANDY V. ZAMORANOS
Independent Director

ROMEO C. DIOLATA
Director

COMMONWEALTH INSURANCE COMPANY
10th, 12th, & 19th/F, BDO Plaza, 8737 Paseo De Roxas, Makati City
info@cic.com.ph cs@cic.com.ph 88187626 / 77500538

SECRETARY'S CERTIFICATE

KNOW ALL MEN BY THESE PRESENTS:

I, LOURDES M. CORCELLES, of legal age, Filipino, with office address at 10th/F, BDO Plaza, 8737 Paseo De Roxas, Makati City, after having been duly sworn in accordance with law, under oath depose and state that:

That I am the duly elected Corporate Secretary of COMMONWEALTH INSURANCE COMPANY (CIC for short), a corporation duly organized and existing under Philippine laws with principal office address at 10th, 12th, &19th Floors, BDO Plaza 8737 Paseo De Roxas, Makati City;

As Corporate Secretary, I am the custodian of corporate records and minutes of the meetings held;

That during the special meeting of the Board Of Directors of the Company held on September 19, 2022 at its Head Office Conference Room where a quorum was present and acting, the majority of the Board of Directors, on motion duly seconded, the following resolution was unanimously adopted and approved, to wit:

"BOARD RESOLUTION"

"RESOLVED, as it is hereby resolved that the updated company's "MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION PROGRAM" as of September 2022 is hereby approved in compliance with the Insurance Commission Circular Letter No. 2019-65 dated November 22, 2019 in relation to AMLC Regulatory Issuance (ARI) A, B, and C, No. 2 s. 2018, and, AMLC Regulatory Issuance (ARI) No. 6 s. 2021."

"RESOLVED FURTHER, that the aforementioned "Money Laundering and Terrorism Financing Prevention Program" be submitted to the Insurance Commission AML Division and to be included in the DIGICUR STATUS REPORT (QUADSREC)".

IN WITNESS WHEREOF, I have hereunto set my hand this 21st day of September, 2022, at Makati City, Philippines.

LOURDES M. CORCELLES
Corporate Secretary

REPUBLIC OF THE PHILIPPINES)
CITY OF MANDALUYONG) S.S.

SUBSCRIBED AND SWORN to before me this 21st day of September, 2022 affiant exhibited to me his/her competent proof of identity, to wit: SSS No.03-6854879-6 & TIN No.123-127-615-000.

ATTY. JUAN JAIME D. NOLASCO
Notary Public
Valid until Dec. 31, 2022
IBP No.171577 – 1/3/2022
PTR No.4863719- 1/3/2022
MCLE No. VI-0020547-4/14/2022
Roll No. 60888
Unit 3F, CSV Bldg., Maysilo Circle,
Mandaluyong City

Doc. No. 413;
Page No. 83;
Book. No. 44;
Series of 2022.