CENTURY PROPERTIES

Creating New Generation Real Estate

Money Laundering and Terrorism Financing Prevention Program (MTPP)

TABLE OF CONTENTS

PART 1: OVERVIEW

I. Introduction

Century Properties Group, Inc. (**"CPGI"**) is one of the leading real estate companies in the Philippines with a 34-year track record. It is primarily engaged in the development, marketing, and sale of mid and high-rise condominiums and single detached homes, leasing of retail and office space, and property management.

Currently, CPGI has six principal subsidiaries through which it develops, markets, and sells residential, office, medical and retail properties in the Philippines, as well as manages residential and commercial properties in the Philippines.

In 2021, CPGI, as a real estate company, was included in the list of Covered Persons under the Republic Act ("**R.A.**") 11521, dated 29 January 2021. As such, the Anti-Money Laundering Council (**"AMLC"**) comprised of the Bangko Sentral ng Pilipinas (**"BSP"**), Securities and Exchange Commission (**"SEC"**) and Insurance Commission (**"IC"**) provided rules and regulations to covered institutions relative to the implementation of R.A. 9160 also known as The Anti-Money Laundering Act of 2001, as amended by R.A. 9194, R.A. 10167, R.A. 10365, R.A. 10927 and R.A. 11521 (the **"AMLA"**) and R.A 10168 also known as The Terrorism Financing Prevention and Suppression Act of 2012 (the **"TFPSA"**). This Manual also considers the updated AMLA and TFPSA Rules and Regulations under AMLC Regulatory Issuance No. 03 Series of 2021, dated 26 May 2021, on 2021 Anti-Money Laundering/Counter-Terrorism Financing (**"AML/CTF"**) Guidelines for Designated Non-Financial Businesses and Professions.

This Manual is designed to ensure that all operating units of the organization and its service providers shall comply with the Anti-Money Laundering and Counter-Terrorism Financing requirements and obligations set out in Philippine legislation, rules, regulations, government regulatory bodies and agencies' guidance, global best practices; and that adequate systems and controls are in place to mitigate the AML risks and that the organization is not used to facilitate financial crime.

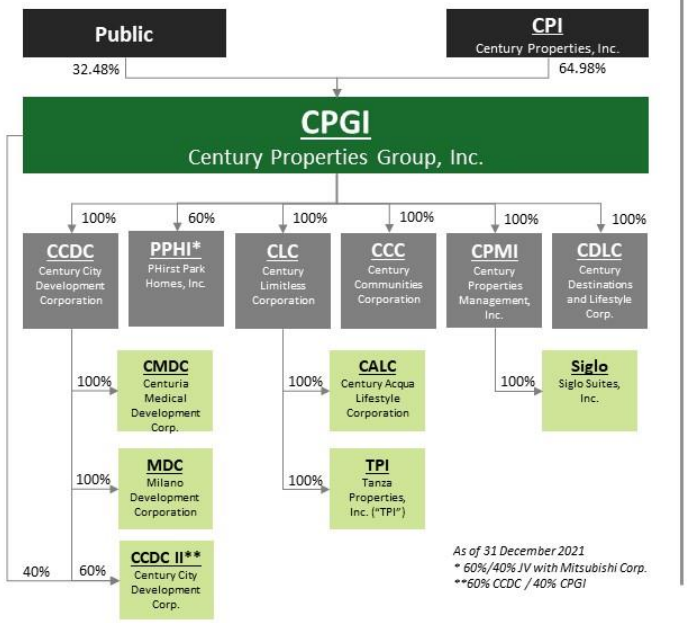
II. Company Profile and Organizational Structure

CPGI formerly East Asia Power Resources Corporation ("EAPRC"), was originally incorporated on March 23, 1975 as Northwest Holdings and Resources Corporation. In September 26, 2011, the Board of Directors of CPGI approved the change in the company's corporate name to its present name, as well as the change in its primary business purpose from power generation to that of a holding company and real estate business. Between May and November 2011, Century Properties Inc. (CPI) entered into a series of transactions with EAPRC, a corporation organized under the laws of the Philippines and listed on the Philippine Stock Exchange, whereby, among other things, CPI acquired 96.99% of EAPRC's Common Shares and EAPRC acquired all of the subsidiaries of CPI.

CPGI has five wholly-owned subsidiaries namely Century City Development Corporation, Century Limitless Corporation, Century Communities Corporation, Century Properties Management and Century Properties Hotel and Leisure Inc. Through these subsidiaries, Century develops, markets and sells residential, office, medical and retail properties in the Philippines, as well as manages residential and commercial properties in the Philippines.

As a member of the Philippine Chapter of the Asia Pacific Real Estate Association, Century Properties is committed to apply industry best practices in the conduct of its business and to continuously work with peers in elevating the standards of the local real estate industry.

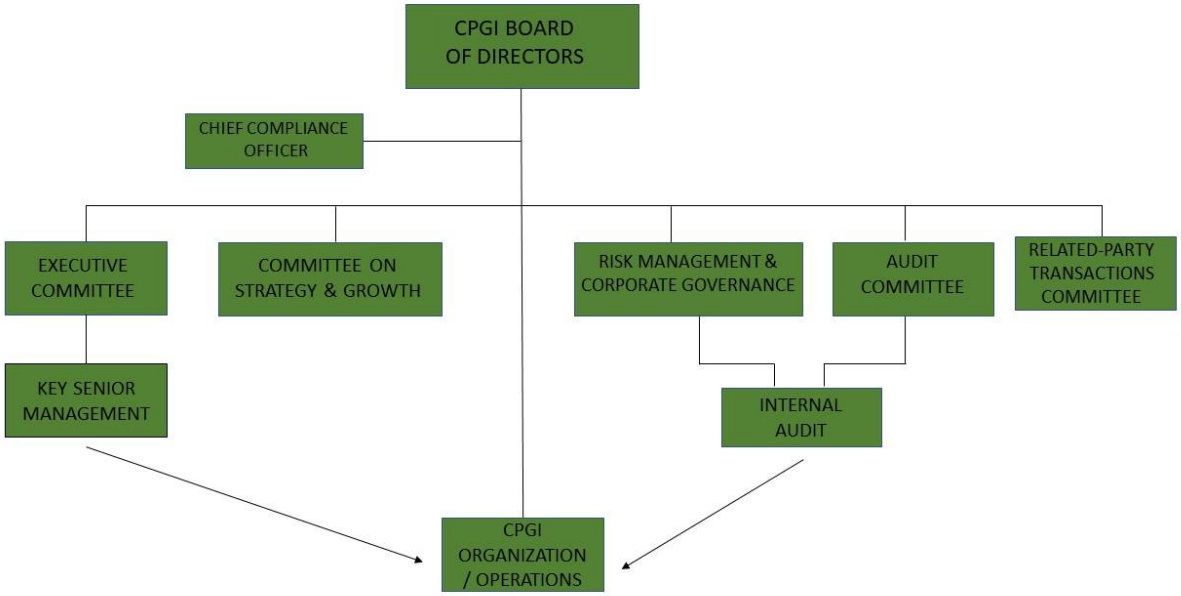
CPGI STRUCTURE AND BUSINESS SEGMENTS



PLATFORMS AND PRODUCTS

In-City Vertical Developments	Mixed-use development consisting of condominium and residential projects
Horizontal Affordable Housing	Affordable high-quality horizontal projects
Commercial Leasing	Retail mall, office buildings, medical facilities
Property Management	Property management; Exclusive, specialty management and leasing service

1



III. Legal Framework

i. Money Laundering and its Stages

Money laundering is the criminal practice of processing ill-gotten gains, or "dirty" money, through a series of transactions; in this way the funds are "cleaned" so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Although money laundering is a diverse and often complex process, it basically involves three independent stages, namely: placement, layering and integration that can occur simultaneously:

Placement. The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a canceled vacation package or purchasing a series of monetary instruments (e.g., cashier's checks or money orders) that are then collected and deposited into accounts at another location or financial institution.

Layering. The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in one or more financial institutions.

Integration. The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a believable explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

ii. Terrorist Financing

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations.

Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds, and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers. There is also evidence that some forms of informal banking have played a role in moving terrorist funds.

Transactions through informal banking are difficult to detect given the lack of documentation, their size, and the nature of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.

IV. Policy Statement

CPGI adopts the policy of the State under AMLA and TFPSA to protect and preserve the integrity and confidentiality of its accounts and to ensure that the Philippines shall not be used as a money laundering site for the proceeds of any unlawful activity. CPGI further supports the State's policy to protect life, liberty and property from acts of terrorism and to condemn terrorism and those who support and finance it and reinforce the fight against terrorism by criminalizing the financing of terrorism and related offenses. Consistent with its policy, CPGI therefore applies the following principles throughout its business:

- Conform with high ethical standards and observe good corporate governance;

- Know sufficiently its Customers and Clients to prevent criminal elements and suspicious individuals or entities from transacting with, or establishing or maintaining relationship with CPGI;
- Adopt and effectively implement an appropriate AML/CTF risk management system that identifies, understand, assesses, monitors, and controls risks associated with money laundering and terrorist financing (**"ML/TF"**);

- Comply fully with existing laws and regulations aimed at combating money laundering and terrorist financing by making sure that CPGI's officers and employees are aware of their respective responsibilities and carry them out in accordance with a superior and principled culture of compliance;

Cooperate fully with the AMLC for the effective implementation of the AMLA and TFPSA and directives and guidance from the AMLC and relevant government agencies.

V. Policy Objectives

CPGI shall implement internal policies, controls and procedures on the following:

a. Risk assessment and management;

b. Detailed procedures of CPGI's compliance and implementation of CDD, record-keeping and Transaction reporting requirements;

c. An effective and continuous AML/CTF training program for all directors and responsible officers and employees, to enable them to full comply with their

obligations and responsibilities under the AML/CTF Laws, their respective IRRs, the AML/CTF Guidelines for Designated Non-Financial Businesses and Professions and other applicable SA and AMLC issuances, their own internal policies and procedures, and such other obligations as may be required by the SA and/or the AMLC;

d. An adequate risk-based screening and recruitment process to ensure that only qualified and competent personal with no criminal record or integrity-related issues are employed or contracted by CPGI;

e. Independent audit function to test the system. CPGI shall specify in writing the examination scope of independent audits, which shall include evaluation or examination of the following:

    1. Risk assessment and management;

    2. MTPP; and

    3. Accuracy and completeness of customer identification information, covered and STRs, and all other records and internal controls pertaining to compliance with the AML/CTF Laws, their respective Implementing Rules and Regulations, the AML/CTF Guidelines for Designated Non-Financial Businesses and Professions and other relevant SA and AMLC issuances.

f. A mechanism that ensures all deficiencies noted during inspection and/or regular or special compliance checking are immediately and timely corrected and acted upon;

g. Cooperation with the SA, AMLC and other competent authorities;

h. Designation of a Compliance Officer at the management level, as the lead implementer of CPGI's compliance program or creation of compliance unit;

i. The identification, assessment and mitigation of ML/TF risks that may be arise from new business practices, services, technologies and products;

j. Adequate safeguards on the confidentiality and use of information exchange, including safeguards to prevent tipping off;

k. A mechanism to comply with freeze, inquiry and asset preservation orders and all directives of the AMLC;

l. A mechanism to comply with the prohibitions from conducting Transactions with designated persons and entities, as set out in relevant United Nations Security Council Resolutions (UNSCRs) relating to the preservation and suppression of terrorism financing and financing of proliferation of weapons of mass destruction.

VI. Policy Scope

This Manual shall apply to CPGI, its existing and future branches, including affiliates supervised and regulated by the AMLC under existing regulation. The scope of the money laundering prevention program shall also extend to combating terrorist financing.

VII. Definition of Terms

a. **"Account"** refers to a business relationship between CPGI and its customer or client.

b. **"AMLA"** refers to Republic Act (RA) No. 9160, as amended by RA Nos. 9194, 10167, 10365, 10927, 11521 or other laws that may subsequently amend the AMLA.

c. **"AMLC"** refers to the Philippines' central AML/CTF authority and financial intelligence unit, which is the government instrumentality mandated to implement the AMLA and TFPSA. It also refers to the official name of the Council, which is the governing body of the said government agency.

d. **"Average Due Diligence" ("ADD")** refers to the normal level of customer due diligence that is appropriate in cases where there is normal risk of money laundering or terrorism financing.

e. **"Beneficiary Financial Institution"** refers to the financial institution, which receives the wire transfer from the originating/ordering financial institution, directly or through an intermediary financial institution, and makes the funds available to the beneficiary.

f. **"Covered Transaction" ("CT")** refers to a cash transaction with or involving CPGI exceeding Seven Million Five Hundred Thousand Pesos (P7,500,000.00) or its equivalent in any other currency.

g. **"Covered Transaction Report" ("CTR")** refers to a report on a CT, as herein defined, filed by a covered person before the AMLC.

h. **"Customer or Client"** refers to any person or entity who keeps an account, or otherwise transacts business with CPGI. 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; and

2. Transactors, agents and other authorized representatives of beneficial owners.

i. **"Customer Due Diligence" ("CDD")** refers to the procedure of identifying and verifying the true identity, of customers, and their agents and beneficial owners, including understanding and monitoring of their transactions and activities.

j. **"Customer Identification Process" ("CIP")** refers to the process of determining the identity of the customer vis-à-vis the valid and acceptable identification document submitted to, and/or presented before CPGI.

k. **"Enhanced Due Diligence" ("EDD")** refers to the enhanced level of scrutiny intended to provide a more comprehensive understanding of the risks associated with the client, as well as confirmation of factual information provided by the client, to mitigate risks presented.

l. **"Financing of terrorism"** is 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 terrorist act; (2) by a terrorist organization, association or group; or (3) by an individual terrorist.

m. "**Identification Document" ("ID")** includes any of the following documents:

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

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

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

    iii. Covered persons registered with and supervised or regulated by the Bangko Sentral ng Pilipinas, Securities and Exchange Commission or Insurance Commission; or

    iv. Philippine Statistics Authority (PSA) under the Philippine Identification System (PhilSys).

2. For foreign nationals: Passport or Alien Certificate of Registration;

3. Other identification document that can be verified using reliable, independent source documents, data or information.

n. **"Institutional Risk Assessment"** refers to a comprehensive exercise to identify, assess and understand a covered person's ML/TF threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and Transactions.

o. **"Monetary Instrument"** refers to:

1. Coins or currency of legal tender in the Philippines, or in any other country;

2. Negotiable checks, such as personal checks and bank drafts; and

3. Other similar instruments where title thereto passes to another by endorsement, assignment or delivery.

p. **"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:

1. Transacts said monetary instrument or property;

2. Converts, transfers, disposes of, moves, acquires, possesses or uses said monetary instrument or property;

3. Conceals or disguises the true nature, source, location, disposition, movement or ownership of or rights with respect to said monetary instrument or property;

4. Attempts or conspires to commit money laundering offenses referred to in "1", "2" or "3" above;

5. Aids, abets, assists in or counsels the commission of the money laundering offenses referred to in "1", "2", or "3" above; and

6. Perform or fails to perform any act as a result of which he facilitates the offense of money laundering referred to in items "1", "2", or "3" above.

Money laundering is also committed by any covered person who, knowing that a covered or ST is required to be reported to the AMLC under any of the provisions of the AMLA, as amended, its Revised Internal Rules and Regulations (**"RIRR"**), fails to do so.

q. **"Money Laundering/Terrorism Financing Prevention Program" ("MTPP" or "Manual")** refers to CPGI's comprehensive, risk-based, and written internal policies, control and procedures to implement the relevant laws, rules and regulations, and best practices to prevent and combat ML/TF and associated unlawful activities in the operational level.

r. **"Monetary instrument or property related to an unlawful activity"** refers to all proceeds, instrumentalities and monetary instruments of an unlawful activity.

s. **"National Risk Assessment" ("NRA")** refers to a comprehensive exercise to identify, assess and understand a country's ML/TF threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions.

t. **"On-going Monitoring Process" ("OMP")** refers to the process of conducting continuing due diligence, including continually assessing the risks, understanding the transactions and activities, and updating, based on risk and materiality, the identification information and/or identification documents, of customers, their agents and beneficial owners.

u. **"Person/Entity"** refers to any natural or juridical person.

v. **"Philippine Identification Card" ("PhilID")** refers to the non-transferrable identification card issued by the Philippine Statistics Authority (PSA) to all citizens and resident aliens registered under the Philippine Identification System. It shall serve as the official government-issued identification document of cardholders in dealing with all government agencies, local government units, government and controlled corporations, government financial institutions, and all private sector entities.

w. **"Politically Exposed Person" ("PEP")** refers to an individual who is or has been entrusted with prominent public position in (1) 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 PEP shall include immediate family members, and close relationships and associates that are reputedly known to have: (1) Joint beneficial ownership of a legal entity or legal arrangement with the main/principal PEP; or (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;

Close relationship/associates of PEPs refer to persons who are 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.

x. **"Proceeds"** refers to an amount derived or realized from any unlawful activity.

y. **"Real Estate"** refers to the land and all those items which are attached to the land. It is the physical, tangible entity, together with all the additions or improvements on, above or below the ground.

z. **"Real Estate Developer"** refers to any natural or juridical person engaged in the business of developing real estate development project for his/her or its own account and offering them for sale or lease.

aa. **"Reduced Due Diligence" ("RDD")** refers to the lowest level of CDD that is appropriate in cases where there is low risk of money laundering or terrorism financing.

bb. **"Risk"** refers to risk of loss arising from ML/TF activities.

cc. **"Risk-Based Approach"** refers to the process by which countries, competent authorities, and covered persons identify, assess, and understand the ML/TF risks to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk. This includes prioritization and efficient allocation of resources by the relevant key players and stakeholders in applying AML/CTF measures in their operations in a way that ensures that they are commensurate with the risks involved.

dd. **"Sectoral Risk Assessment"** refers to a comprehensive exercise to identify, assess and understand an industry's, or business or professional sector's, threats, vulnerabilities and the consequential risks, with a view to mitigate illicit flow of funds and transactions.

ee. **"Source of Fund"** refers to the origin of the funds or other monetary instrument that is the subject of the transaction or business or professional relationship between a CPGI and the customer.

ff. **"Source of Wealth"** refers to the resource from which the customer's wealth, including all monetary instruments and properties, came, comes, or will come from, such as employment, business, investment, foreign remittance, inheritance, donation, and winnings.

gg. **"Supervising Authority" ("SA")** refers to the BSP, the SEC, the IC, or other government agencies designated by law to supervise or regulate a particular financial institution or Designated Non-Financial Businesses and Professions.

hh. **"Suspicion"** refers to a person's state of mind—based on his skills, experience, and/or understanding of the customer profile—which considers that there is a possibility that any of the suspicious circumstances exists.

ii. "**Suspicious Transaction" ("ST")** refers to a Transaction with CPGI, regardless of the amount involved, where any of the following circumstances exists:

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 AMLA;

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 CPGI;

6. The transaction is in any way related to an unlawful activity or any money laundering activity or offense, that is about to be committed, is being or has been committed; or

7. Any transaction that is similar, analogous or identical to any of the foregoing.

Any unsuccessful attempt to transact with CPGI, the denial of which is based on any of the foregoing circumstances, shall likewise be considered as ST.

Per Implementing Rules and Regulations **("IRR")** of R.A. 10168 rule 3.a.15, in determining whether a Transaction is suspicious, CPGI considers 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. Client was reported and/or mentioned in the news to be involved in terrorist activities;

4. Client is under investigation by law enforcement agencies for possible involvement in terrorist activities;

5. Transactions of individuals, companies or Non-government Organizations (NGOs)/ non-Profit Organization (NPOs) that are affiliated or related to people suspected of having connected with a terrorist individual, organization or group of persons;

6. Transactions of individuals, companies or NGOs/NPOs that are suspected of being used to pay or receive funds from a terrorist individual, organization or group of persons;

7. It includes attempted transactions made by suspected or designated terrorist individuals, organizations, associations or group of persons.

Per AMLC Regulation Issuance No. 3, in determining whether a transaction is suspicious, CPGI considers the following circumstances:

1. Wire significant and unexplained geographic distance between the agent and the location of the customer and property.

2. Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interest.

3. The use of intermediaries with no clear or definite relationship.

4. Buying and selling transactions that have no clear economic reason.

5. When the customer invests in the real estate market but the purchase or sale prices are not commensurate with the real estate value.

6. When a customer instructs to sell assets or real estate properties repeatedly without realizing any profit margin or submitting a reasonable explanation in this respect.

7. When a customer uses another person as a façade to complete a transaction without any legitimate financial, legal or commercial excuse.

8. When the customer does not indicate concern in incurring losses or realizing extremely low profits in comparison with persons engaged in the same business, or when the customer remains persistent in pursuing his activities.

9. Cash transactions in large amounts, including foreign exchange transactions or cross-border fund movement, if such types of transactions are not consistent with the usual commercial activity of the customer.

10. When the customer has an unusually comprehensive knowledge of money laundering and terrorism financing issues and the AMLA, and the TFPSA

without any justification, as when the customer points out he wishes to avoid being reported.

11. When the customer attempts to divide the amounts of any operations below the applicable designated threshold of reporting to the competent authorities regarding ML and TF suspicions.

12. When the customer has an unusual interest in the internal policies, controls, regulations and supervisory procedures and unnecessarily elaborates on justifying a Transaction.

13. When a customer has accounts with several international banks or has lately established relationships with different financial institutions in a specific country without clear grounds, particularly if this country does not apply an acceptable AML/CTF regime.

14. When the customer is reserved, anxious or reluctant to have a personal meeting.

15. When the customer uses different names and addresses.

16. When the customer refuses to submit original documentation particularly those related to his identification.

17. When the customer intentionally conceals certain important information like his address (actual place of residence), telephone number or gives a non-existent or disconnected telephone number.

18. When the customer uses a credit card issued by a foreign bank that has no branch or headquarters in the country of residence of the client while he does not reside or work in the country that issued said card.

19. When the customer conducts cash transactions where banknotes with unusual denominations are used.

20. When the customer conducts unusual transactions in comparison with the volume of the previous transactions or the activity pursued by the Customer.

21. When the customer conducts unnecessarily complex transactions or those that may not be economically feasible.

22. When the customer's transaction involves a country that does not have an efficient AML/CTF regime, or is suspected to facilitate ML/TF operations. or where drug manufacturing or trafficking are widespread.

jj. **"Suspicious Transaction Report" ("STR")** refers to a report on a ST, as herein defined, filed by a covered person before the AMLC.

kk. **"Transaction"** refers to any act establishing any right or obligation or giving rise to any contractual or legal relationship between CPGI and its customer. It also includes any movement of funds, by any means, in the ordinary course of business with CPGI.

ll. **"Unlawful activity"** refers to any act or omission 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, 11, 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, 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. No. 455 and Republic Act. No. 1937, as amended, otherwise known as 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, otherwise known as the "Anti-Hijacking Law"; "Destructive Arson"; and "Murder", as defined under the Revised Penal Code, as amended;

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 R.A. 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 IV, 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 R.A. 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 R.A. No. 8042, otherwise known as the Migrant Workers and Overseas Filipinos Act of 1995;
29. Violation of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines, as amended;

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 nature similar to the aforementioned unlawful activities that are punishable under the penal laws of other countries.

PART 2: GOVERNANCE AND OVERSIGHT

I. Insitutional Risk Assessment and Management

CPGI shall develop sound risk management policies and practices to ensure that risks associated with ML/TF such as counterparty, reputational, operational and compliance risks are identified, assessed, monitored, mitigated andcontrolled, as well as to ensure effective implementation of this Manual, to the end that CPGI shall not be used as a vehicle to legitimize proceeds of Unlawful Activity or to facilitate or finance terrorism.

The four (4) areas of sound risk management practices are adequate and active board and senior management oversight, acceptable policies and procedures embodied in a ML/TF prevention compliance program, appropriate monitoring and comprehensive internal controls and audit.

i. Risk Assessment

CPGI shall:

- Take appropriate steps to identify, assess and understand its ML/TF 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.

- Institute the following processes in assessing their ML/TF risks:

    - Documenting risk assessments and findings;

    - Considering all the relevant risk factors, including the results of NRA and Sectoral Risk Assessment, before determining what is the level of overall risk and appropriate level and type of mitigation to be applied;

    - Keeping the assessment up-to-date through periodic review; and

    - Ensure submission of the risk assessment information as may be required by the SA.

- Maintain ML/TF prevention policies, procedures, processes and controls that are relevant up-to-date in line with the dynamic risk associated with its business, products and services and that of its customers.

- Establish, implement, monitor and maintain satisfactory controls that are commensurate with the level of ML/TF risk and take enhance measures on identified high risk areas, which should be incorporated in the CPGI's MTPP.

- Conduct additional assessment as and when required by the SA; and

- Institutional Risk Assessment shall be conducted at least once every two (2) years, or as often as the Board of Directors or senior management may direct, depending on the level of risks identified in the previous assessment, or other relevant ML/TF developments that may have an impact on CPGI's operation.

ii. Risk Management

CPGI shall:

a. Develop sound risk management policies, controls and procedures which are approved by the Board of Directors, to enable them to manage and mitigate the risks that have been identified in the NRA, or by the AMLC, the SA or CPGI itself;

b. Monitor the implementation of those controls and to enhance them if necessary; and

c. Take enhanced measures to manage and mitigate the risks where higher risks are identified.

The Board of Directors of CPGI shall exercise active control and supervision in the formulation and implementation of institutional risk management.

II. Corporate Governance

As mandated by Section 2.2, Rule 4 of 2018 IRR of AMLA as amended, CPGI's Board of Directors shall be ultimately responsible for its compliance with the AMLA and TFPSA, their respective IRRs, and other AMLC issuances.

The Board of Directors shall ensure that CPGI will not be used as a site or a party of ML/TF.

The Board of Directors shall appoint a Compliance Officer that shall directly report as regards the day-to-day Transaction or any concerns arising in relation to ML/TF. Should the Board of Directors delegate audit, whether announced or unannounced, the auditor, both internal and external, shall directly report to the Board of Directors.

The Board of Directors shall approve manuals, prevention programs and policies, to strengthen the steps taken, in relation to money laundering and terrorism financing and shall exercise active oversight together with the Compliance Officer who will be the lead implementer.

The manual and programs are also applicable and must be followed by all branches.

III. Compliance Management

The Compliance Officer shall directly report to the Board of Directors of CPGI or any board- level or approved committee on all matters involving money laundering and combatingterrorism.

The Compliance Officer shall also ensure that compliance measures reflect readily available information concerning new trends in ML/TF and detection techniques.

The Compliance Officer shall be principally responsible for the following functions among other functions that may be delegated by senior management and the Board of Directors, to wit:

- Ensure compliance by all responsible officers and employees with this Guidelines, the AML/CTF Laws, their respective IRRs, other directives, guidance and issuances from the SA and AMLC. It shall 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/TF prevention, reporting channels, effectiveness of AML/CTF transaction monitoring system and record retention system through sample testing and review of audit or checking reports. It shall also report compliance findings to the Board of Directors.

- Ensure that infractions, discovered either by internally initiated audits, or by special or regular compliance checking conducted by the SA and/or AMLC are immediately corrected;

- Inform all responsible officers and employees of all resolutions, circulars and other issuances by the SA and/or the AMLC in relation to matters aimed at preventing ML and TF;

- Alert senior management and the Board of Directors if s/he believes that CPGI is failing to appropriately address AML/CTF issues; and

- Organize the timing and content of AML/CTF training of officers and employees including regular refresher trainings.

The qualifications of a Compliance Officer are as follows:

- Must be a senior level officer of the company; and

- Directly reporting to the Board of Directors.

IV. Internal Controls and Audit

In order to preserve the integrity of the program in relation to AML/CTF and the risk management framework, the internal audit team shall, from time-to-time, conduct an in-depth audit to check whether the Departments and or employees involved are following the policies and programs as stated herein and to test the effectiveness of the policies and programs. The independent internal audit examination shall be conducted at least once every 2 years or at such frequency as necessary.

The internal audit shall directly report to the Board of Directors in relation to the result of its audit. In cases of high risk ST and ST, it must be reported to the Board of Directors immediately to avoid tipping off.

CPGI shall establish internal controls to ensure day-to day compliance with its AML/CTF obligations under the AML/CTF laws, their respective IRRs, the AML/CTF Guidelines for Designated Non-Financial Businesses and Professions, and other applicable SA and AMLC issuances, taking into consideration the size and complexity of its operation.

Members of the Division Heads, Department Heads, and all Officers are responsible for ensuring that employees adhere consistently to the AML policies and procedure to prevent ML/TF.

V. Hiring Policies and Procedures

CPGI aims to have all its employees knowledgeable as regards AMLA and TFPSA especially its front liners in dealing with Clients. Employees should carry out their duties in accordance with the MTPP.

CPGI aims to take measure in hiring employees to ensure that it is not related or involved in any money laundering business or a member of any organization supporting terrorism by doing the following:

- Background checking which includes the immediate family, the current residence and other closely related persons to the employee hired or to be hired.
- Confirming education attainment and previous employment.

CPGI will also conduct training of employees, at least twice (2) a year in order to ensure the following:

- Role of Board of Directors, Officers and Employees in relation to AML/CTF
- Risk Management
- Preventive Measures

- Compliance to AMLC's directive and issuances
- Reporting and Coordination with AMLC

PART 3: POLICIES AND PROCEDURES

I. Customer Acceptance and Due Diligence

1. Customer Identification/ Know-Your Customer

In order to comply with the requirements of AMLC as regards accepting Clients, the following are the standards that will be implemented by CPGI in relation to accepting new Clients or renewal of Clients, businesses or partnership with CPGI:

- It shall be the policy of CPGI for all clients, regardless of the nature of Transaction, to require the risk-based and tiered policy;
- In all instances, the Company shall document how a specific Customer was profiled (low, normal, or high) and what standard of CDD (reduced average or enhanced) was applied.
- CPGI shall require a more extensive due diligence for high risk Clients, such as those known in public as controversial personalities, those individuals holding high-profile public position or PEPs;
- Decisions to enter into business relationships with high risk Clients shall be taken exclusively by senior management officers or the Board of Directors, on case to case basis considering the Risk;
- It shall be the policy of CPGI not to accept or enter into business relationship with clients, who refuse to produce the required IDs and to discontinue business relationship with Clients, who after a series of follow up requests, failed to submit their IDs.

In designing a customer acceptance policy, the following factors are considered:

- Background and Source of Funds;
- Country of origin and residence or operations;
- Public/high profile position of the Person or its directors/trustees, stockholders, officers and/or authorized signatory;
- Linked accounts;
- Watchlist of individuals and entities engaged in illegal activities or terrorist related activities as circularized by BSP, AMLC, and the 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 CPGI.

2. *Customer Risk Profiling/Assessment*

i. Customer Risk Profiling

It is relevant in CPGI to identify and classify each Clients whether, it is a high, moderate or low risk Clients. The classification of Clients will be the basis for the due diligence required to be observed by its employees.

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

1. Low Risk

Individual Clients:

- Individuals who are able to produce major requirements for identification
- Individuals with confirmed regular employment in a legitimate business or office

Corporate, Partnership or Sole Proprietor Clients:

- Publicly listed companies subject to regulatory disclosure requirements
- Government agencies including GOCCs
- Department of Trade and Industry (**"DTI"**) or SEC-registered company
- Publicly-listed company subject to regulatory disclosure requirements by the SEC/Philippine Stock Exchange
- Registered Partnership
- Registered Association
- Unincorporated company

2. *Normal Risk*

- Individual customer or entities not falling under "Low Risk" or "High Risk"

- Individual/ 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*

- Individuals who are publicly known to be a threat in the Philippines or related by affinity or consanguinity.

- Individuals who are under investigation by the government or under the watch-list of any government agency or any other international agency which are communicated to the Philippine government.

- Individual/Authorized Signatory (in case of Corporation) who is an incumbent PEP:

    - National and Local Government Officials
    - Head of Foreign State
    - Judicial Officials
    - Uniformed Personnel.
    - Appointive Government Officials: Cabinet Secretary and Undersecretary
    - Head of Government Owned or Controlled Corporations
    - Leaders of major National Political Parties

    *A Barangay Chairman may be considered as PEP but may not be a high risk, except if it has assets which are unexplainable or not commensurate with his status or source of income.

- Those who are nationals or citizens from foreign jurisdiction or geographical location that presents greater risk for ML/TF or its associated Unlawful Activities or is recognized as having inadequate internationally accepted AML/CTF standards, as determined by domestic or international bodies.

ii. Client Assessment Procedure[1]

1. The front-liner Account Officer shall determine classification by assessing the client as provided above, whether it is a low, normal or high risk.

[1] Attached as Annex "A" Risk Assessment Form

2. Before entering into a Transaction, the Account Officer shall also check the name of the Client or broker if it is one of the names under the watchlist of any government agencies or the AMLC.

3. After determining the Client classification, the Account Officer shall require Client to submit information and IDs according to the level of required CDD.

3. Customer Verification

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

For New Individual Clients:

1. Full Name of Client;
2. Date and Place of birth;
3. Name of beneficial owner, if applicable;
4. Present Address;
5. Permanent Address;
6. Contact Number or information;
7. Nationality;
8. Specimen Signature or biometrics of the Customer;
9. Proof of Identification and Identification number;
10. Nature of work and name of employer or nature of self-employment/business, if applicable;
11. Source of Funds or property; and
12. TIN, SSS or GSIS, if applicable.

CPGI shall also verify the identity of any person purporting to act on behalf of the Customer and whether or not he is so authorized by the Customer.

Corporate, Partnership and Sole Proprietor Clients

Minimum Information:

1. Name of entity;

2. Name, present address, date and place of birth, nationality, nature of work and Source of Funds of the beneficial owner, if applicable, and authorized signatories;

3. Official address;

4. Contact number or information;

5. Nature of business;

6. Specimen signature or biometrics of the authorized signatory;

7. Verified identification of the entity as a corporation, partnership, sole proprietorship;

8. Verified identification of the entity's Source of Funds and business nature of the entity;

9. Verification that the entity has not been or is not in the process of being dissolved, struck-off, wound-up, terminated, placed under receivership , or undergoing liquidation; and

10. Verifying the relevant supervisory authority the status if the entity.

Corporate Documents:

1. Certificates of registration issued by the DTI for sole proprietorship and SEC for corporation and partnership;

2. Secondary License or Certificate of Authority issued by the SA or other government agency;

3. Articles of Incorporation or Association and By-laws;

4. Latest General Information Sheet which list the names of directors/trustees/partners, principal stockholders owning at least 25% of the outstanding capital stock and primary officers. (President, Treasurer. etc.)

Identification documents of the owners, partners, directors, principal officers,

authorized signatories and stockholders owning at least 25% of the business of outstanding capital stock, as the case may be.

For entities registered outside the Philippines, similar documents and/or information duly authenticated by 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.

Face-to-Face contact. There must be a face-to face contact with the Clients. Without such, no Transaction shall be processed. However, the use of Information and Communication Technology may be allowed, provided that CPGI is in possession of and has verified the IDs submitted by the protective customer prior to the interview and that the entire procedure is documented.

4. Identification and Verification of Agents

CPGI shall undertake satisfactory Customer Due Diligence measures:

- Before establishing business relationship;
- There is any suspicion of ML/TF; and
- There is doubt about the integrity or adequacy of previously obtained Customer identification information.

Provided, that where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, CPGI may complete verification after the establishment of business relationship so as not to interrupt normal conduct of business. The verification of the identity of the customer shall be conducted within the duration of the policy/plan/agreement or at the time the customer files his/her claim, as the case may be.

The Account Officer or Deparrment shall comply with the following guidelines for establishing the true and full identity of the Clients:

a) Reduced Due Diligence (RDD) for Low Risk Clients

CPGI shall observe the following:

i. For individual Clients, upon presentation of acceptable IDs as defined in this Manual or other reliable, independent source documents, data or information may avail of the products of CPGI.

ii. For corporate, partnership, and sole proprietorship entities, upon submission of the required documents may avail of the products of CPGI.

b) Average Due Diligence (ADD) for Normal Risk Clients and for New Individual/Corporate Clients

New Individual Client: CPGI shall obtain at the time of Transaction all the minimum information and confirming this information with the valid IDs hereof from individual Clients before establishing any business relationship.

New Corporate and Juridical Client: CPGI 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 (EDD) for High Risk Clients[2]

CPGI shall do the following as EDD:

1. Obtain additional information other than the minimum information and/or documents required for the conduct of ADD;

   (a) In cases of individual Clients:

      i. Supporting information on the intended nature of the business relationship/Source of Funds/Source of Wealth,

      ii. Reasons for the intended or performed Transactions,

      iii. List of companies where he is a director, officer or stockholder,

      iv. List of banks where the individual has maintained or is maintaining an account, and

      v. Other relevant information available through public databases or internet.

   (b) For entities assessed as high risk Clients, 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 Funds of each of the

[2] Attached as Annex "B" Enhanced Due Diligence Forms for Individual/Legal Entity

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 Board Committee approval to commence business relationship.

4. Conduct enhanced OMP of the business relationship.

5. 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, CPGI shall deny business relationship with the Client without prejudice to the filing of STR to the AMLC when so warranted.

6. In addition to profiling of clients 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 Account Officer or Deparment has obtained the abovementioned additional information and/or documents from its Clients and has secured senior officer's approval.

Enhanced Due Diligence, Minimum Validation

Individual Clients – Validation procedures include but are not limited to the following:

1. Confirming the date of birth from a duly authenticated official document.

2. 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.

3. Contacting the Customer by phone or email.

4. Determining the authenticity of the IDs through validation of its issuance by requesting a certification from the issuing authority or by any other effective and reliable means. Determining the veracity of the declared Source of Funds.

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

1. Validating the source of funds or Source of Wealth from reliable documents such as Audited Financial Statements, Income Tax Return, bank references, etc.

2. Inquiring from the supervising authority the status of the entity.

3. Verifying the address through on-site visitation of the company, sending thank you letters, or other documents showing address.

4. Contacting the entity by phone or email.

*** High Risk Client – A Client that is from a foreign jurisdiction and recognized as having inadequate internationally accepted AML standards, or presents greater risk for ML/TF or its associated unlawful activities, shall be subject to EDD. Information relative to these are available from publicly available information such as the websites of Financial Action Task Force (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.

**** Shell Company/ Shell Bank – CPGI must exercise 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.

5. Beneficial Ownership Verification

Where trusts or similar arrangements are used, or where the customer is a trust, CPGI shall verify the identity of the trustees, any other person exercising effective control over the trust property, the settlors and the beneficiaries.

6. *Determination of the Purpose of Relationship*

Where applicable, the background and purpose of the activity in question may be examined by the Compliance Officer and the findings may be established in writing.

CPGI shall examine the background and purpose of relationship 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.

7. *Ongoing Monitoring of Customer's Information and Accounts/Transactions*

On-going Monitoring Process is an essential aspect of effective KYC procedures. The front-line Account Officers of CPGI, including senior management who are directly in contact with high-net worth Clients shall have an understanding of the normal and reasonable account activity of the clients.

The process of on-going monitoring of Accounts includes the following:

a. Customer information and IDs should be kept up to date once every three (3) years in conformity with the RIRR. A risk-and-materiality based on-going monitoring of Customer's Accounts and Transactions is to be part of CDD.

b. Timely information like reports on critical Customer data not obtained/disclosed despite diligent follow up, or such reports on Clients with unusual activities that may lead to STs shall be provided to the Department copy furnished the Compliance Officer who will analyze and effectively monitor high risk Customer accounts.

c. Members of senior management who are in direct contact with high net worth/important clients shall endeavor to know the personal circumstances of these clients and be alert to sources of third party information. Unusual activities of these types of clients that may put CPGI at risk shall be reported to the AMLC Committee.

Enhanced Due Diligence – CPGI 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.

To this extent, CPGI Enhanced Due Diligence on its customer if it acquires information in the course of its Customer Account or Transaction monitoring that:

a. Raises doubt as to the accuracy of any information or document provided or the ownership of the entity.

b. Justifies reclassification of the Customer from low or normal risk to high-risk pursuant to its own criteria; or

c. Any of the circumstance for the filing of a ST exists.

d. Where additional information cannot be obtained, or any information or document provided is false or falsified, or result of the validation process is unsatisfactory, CPGI shall immediately close the account and refrain from further conducting business relationship with the customer without prejudice to the reporting of a ST to the AMLC when circumstances warrant.

II. Preventive Measures for Specific Transactions and Activities[3]

CPGI shall implement a Comprehensive Compliance Testing Program (**"CCTP"**) to assess its own risk areas. The CCTP shall cover all divisions of CPGI, including its branches which shall be conducted annually.

At the minimum, the scope of the CCTP shall include the following:

- Adoption of the AMLA Manual;
- CDD or Know-Your-Customer ("KYC") Rule;
- Monitoring, Recording and Reporting;
- Internal Control and Procedures, Compliance and Training; and
- Other issues regarding compliance with AML and CTF Laws, implementing Rules and Regulations, SA and AMLC Issuances.

III. Politically Exposed Persons

CPGI 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. PEPs' position and the position's attendant risk with respect to ML/TF shall be carefully considered especially in determining what standard of due diligence shall apply to the same.

[3] Attached as Annex "C" Comprehensive Compliance Testing Program

In case of domestic PEPs or persons who have been entrusted with a prominent function by an international organization, or their immediate family members or close associates, in addition to performing the applicable due diligence measures, CPGI shall:

- Take reasonable measures to determine whether a Customer, and his agent and the beneficial owner are PEPs; and

- In cases when there is a higher business relationship risk, adopt the following measures:

    - Obtain senior management approval before establishing/ refusing or, for existing Customers, continuing, such business relationships;

    - Take reasonable measure to establish the Source of Wealth and the source of funds of Customers and Beneficial Owners identified as PEPs; and

    - Conduct enhanced OMP on that relationship.

In relation to foreign PEPs, in addition to performing the applicable CDD measures, CPGI shall:

- Put in place risk management systems to determine whether a Customer or the beneficial owner is a PEP;

- Seek the approval of the senior management, if necessary, before establishing, or continuing or existing Customers, such business relationship;

- Take reasonable measures to establish the Source of Wealth and the Source of Funds of customers and Beneficial Owners identified as PEP;

- Conduct enhanced OMP on that relationship; and

- Follow the Customer Acceptance Policy.

CPGI shall have clear, written and graduated accepted policies and procedures that will seek to prevent suspicious individuals or entities from transacting with, establishing or maintaining business relationship with them.

If the prospective customer is unable to comply with any of the CDD measures, CPGI shall refuse to commence business relations or perform the Transaction.

IV. Transaction Reporting[4]

[4] Attached as Annex "D" AML/CTF Flow of Reporting of Covered and Suspicious Transactions

CPGI has a system of reporting all CTs and develops a manner of reporting of STs to avoid tipping off. Any member of the management or staff who discovers or suspects fraudulent or other criminal activity, including terrorist financing, must contact the Compliance Officer and complete a STR.[5]

Notification and Reporting of Suspected Criminal activities. Any member of the management or the staff who discovers or suspects fraudulent or other criminal activity/ies, including terrorist financing, must contact the compliance and complete a STR.

CTs and STs. Should a Transaction be determined to be both a CT and ST, the same shall be reported as a ST. In this regard, it shall l be reported first as a CTR, subject to updating if it is finally confirmed to be reportable as STR.

Quality. The reporting shall meet the standard of quality of reporting which are as follows:

- CPGI ensures that all reports are complete, true and timely filed.
- It shall be submitted and addressed to the EXECUTIVE DIRECTOR of AMLC located in BSP, Roxas Boulevard, Manila City.
- Must provide the details as to, 5Ws and 1H (who, what, where, when, why and how), as outlined by the AMLC, to wit:

  Who

  For the subject profile, the data in the name address and date of birth fields are considered essential information for analysis and investigation. Thus, Covered Persons should ensure that these information are provided when filing STRs. In addition, data for the subject of suspicion in the STR should contain the name of the entity or individual suspected to be engaged in the predicate crime and/or money laundering activity.

  What

  The Covered Persons should ensure that the Transaction code field is filled- up with the appropriate code. Additional information, such as the amount and currency code used, should also be provided by the Covered Persons.

  Where

  In order to determine where the place of the ST occurred, AMLC looks for the branch of the Covered Person/reporting institution where the transaction was made. This is the reason why the AMLC requires, under the revised reporting procedure, that all CTRs/STRs must be reported by the branch of Covered

[5] Attached as Annex "E" Procedure for Reporting Covered or Suspicious Transactions

Persons where the transactions occurred. Further, in cases wherein the head office files the CTRs/STRs, the reporting guidelines emphasized that CTR/STR submission should identify the CP up to the branch level.

When

The Transaction date should be provided by the Covered Person.

Why

ST as defined under the AMLA, should be filed by Covered Persons based on its suspicious indicator. In filing an STR, the Covered Persons should be able to properly assess if the activity falls under any of the suspicious indicators or predicate crimes of the AMLA, as amended. Thus, the Covered Persons should be able to indicate the correct suspicious circumstance or predicate crime in relation to the reported transaction.

How

The narrative should describe the basis for suspicion by providing details such as the pattern of transactions and description of the information in the account opening form, nature of business, sources of income, affiliations, internal database alerts on the subject, and open source information, which serve as the foundation that money laundering or terrorism financing has occurred or is about to occur. The Covered Persons should clearly describe the nature of the suspicious activity, taking into account important details such as the pattern of transactions and if available customer due diligence information. It may include the nature of business/profession, sources of income, affiliations, internal database alerts on the subject, open source information, and the like.

1. *Covered Transactions*

   CT shall be filed within five (5) working days, unless the AMLC prescribes a different period not exceeding fifteen (15) working days, from the occurrence thereof. Transactions that are considered as *"non-cash, no/low risk CTs"* are subject to deferred reporting.

2. *Suspicious Transactions*

   ST[6] shall be reported not later than five (5) days after the date of occurrence of facts that may constitute a basis for filing a STR. For STs, "occurrence" refers to the date of determination of the suspicious nature of the Transaction, which determination shall be made not exceeding ten (10) calendar days from the date of Transaction. Additionally, the following rules shall be

[6] Attached as Annex "F" Suspicious Transaction Report Form

observed:

- CPGI shall adopt policies, procedures, processes and controls in place that would enable an employee to report to the Compliance Officer any suspicion or knowledge of ML/TF activity and/or Transaction that is detected or identified;

- It is the duty of every employee to report any ST/s or activity/ies to the Compliance Officer. Reporting should be done using the reporting procedures set out in this section.

- Employees encountering suspicious and/or high risk Transaction should immediately report the same to Compliance Officer.

  Note: No administrative, criminal or civil proceedings shall lie against the employee reporting the ST in the regular performance of his duties of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct.

- All internal reports must reach the Compliance Officer and must not be blocked at the Department level. No administrative sanction shall be imposed against the employee who directly reports CT or ST to the Compliance Officer or Deputy Compliance Officer, if any.

- The Compliance Officer shall promptly file and STR with the AMLC should there be reasonable grounds to suspect that funds concerning an actual or proposed Transaction are the proceeds of any criminal activity or are related to ML/TF.

- The Compliance Officer shall ensure that every employee is aware of his role and duty to receive or submit internal STRs.

- The Compliance Officer shall investigate STRs internally, build an internal report outlining the outcome of his investigation including the decision on whether or not to file an STR with the AMLC; If upon determination that there is a reasonable ground to report the matter as ST, it must be within 10 working days after determination of occurrence.

- The Compliance Officer may discuss the report with senior management or members of the board level committee or Board of Directors.

- Where applicable, the background and purpose of the activity in question may be examined by the Compliance Officer and the findings may be established in writing.

- In the event the Compliance Officer concludes that no external report should be submitted to the AMLC, the justification of such a decision should be documented.

- CPGI shall institute disciplinary measures against any employee who fails to make an internal suspicious activity report where there is evidence for him/her to do so.

- Electronic copies of CTRs and STRs shall be preserved and safely stored for at least five (5) years from the dates the same were reported to the AMLC.

V. Confidentiality and Tipping-off

When reporting covered or STs, CPGI and its directors, officers and employees are prohibited from communicating, directly or indirectly, in any manner or by any means, to any non-authorized person or entity, or to the media, the fact that the same has been or is about to be reported, the contents of the report, or any other information in relation thereto. Any violation will be dealt with in accordance with the AML/CTF Laws or AMLC issuances.

In case where CPGI form a suspicion of ML/TF and associated Unlawful Activities and reasonably believes that performing the CDD process would tip off the customer, CPGI is permitted not to pursue the CDD process. In such circumstances, CPGI may proceed with the Transaction, immediately file a STR with the AMLC, closely monitor the Account, and review the business relationship.

VI. Training and Continuing Education Program

CPGI's Anti-Money Laundering Policy and Procedure shall be included in all orientation programs for newly hired employees, officers and directors.

The education and training programs shall include the following topics:

- Overview on ML/TF and AMLA;

- Roles of Directors, Officers and Employees in ML/TF prevention;

- Risk Management;

- Preventive Measures;

- Compliance with freeze, bank inquiry and asset prevention orders, and all directives of the AMLC;

- Cooperation with the AMLC and the SA; and
- International standards and best practices.

In addition, higher training will also be provided to CPGI's Compliance Officer, Internal Auditors, other Officers and staff responsible for complying with AMLA Procedures and Requirements.

Attendance by CPGI'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 SA and the AMLC, upon request.

A refresher training course shall also be conducted every two (2) years which may include inviting outside resource persons for this purpose.

This Manual shall be posted on the intranet to ensure that all employees and sales force are aware of the provisions of the AMLA and its IRR. Updated guidelines and specific responsibilities with regard to implementation on threshold amounts, verification of Customer's identification, determining Sources of Funds and reporting procedures, etc. will be issued by e-mail and likewise posted on the intranet to ensure that all employees do not forget their reportorial and compliance responsibilities.

In cases where there are new developments brought about by new legislations, rules and regulations, and other SA and/or AMLC issuances, CPGI shall immediately cascade these information to its responsible Directors, Officers, and employees through the intranet system.

VII. Record Keeping and Retention

a. Record Keeping

1. All Customer and Transaction documents of CPGI shall be maintained and safely stored for five (5) years from the date of the Transaction.

2. Client relationships and Transactions shall be properly documented. In this regard, adequate records on customer identification shall be maintained to ensure that:

   i. Any Transaction can be reconstructed and an audit trail is established when there is suspected money laundering; and

   ii. Any inquiry or order from the regulatory agency or appropriate authority can be satisfied within a reasonable time such as disclosure of information (e.g., whether a particular person is the client or beneficial owner).

3. In the instance that 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 Records and Documents – CPGI shall designate at least two (2) Officers who will be jointly responsible and accountable in the safekeeping of all records and documents required to be retained by the AMLA, as amended, its RIRR and this Manual. They shall have the obligation to make these documents and records readily available without delay during SEC/AMLC regular or special examinations.

Records of CTRs and STRs shall be maintained and safekept by CPGI. A register of all reports made to the AMLC, as well as reports made by the directors, officers or employees relative to STs, whether or not such were reported to AMLC, 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 involving the Transaction.

c. Form of Records – Records shall be retained as originals or copies in such forms as are admissible in court pursuant to existing laws, such as the e-commerce act and its IRRs, and the applicable rules promulgated by the Supreme Court. Further, electronic copies of all covered and STRs shall be kept for at least five (5) years from the date of submission to the AMLC.

VIII. Third-Party Reliance

CPGI may rely on a third party in conducting CDD procedures. For this purpose, the third party shall be:

- A covered person; or
- A financial institution operating outside the Philippines that is covered by equivalent CDD and record-keeping procedures.

In cases of high-risk Customers, CPGI relying on the third person shall also conduct EDD procedure.

IX. Outsourcing of Customer Identification and Due Diligence

CPGI may outsource the conduct of CDD and record-keeping to a counter-party intermediary or agent.

New Products and Business Practices. CPGI shall identify and assess the ML/TF risks that may arise in relation to the development of new products and business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

New Technologies. CPGI shall take reasonable measures to prevent the use of new technologies for ML/TF purposes.

X. Customer Refusal

CPGI will not accept as customers or conduct transactions with persons or entities in the following circumstances:

a. The person has been identified by reliable sources as being a criminal or terrorist or being associated with criminal or groups;

b. The person is involved in certain criminal or such other activities that are considered to be of high risk, given the nature of the source of funds;

c. The person is from a jurisdiction which has been identified as an area/country of high risk by the financial intelligence unit and/or supervisory authority;

d. The person is from a jurisdiction identified by reliable sources as one that has high levels of criminal or terrorist activities; and

e. The employee has reason to believe, based on the behavior of the person or other factors that the transaction may be related to money laundering or the findings of terrorism.

XI. Prohibited Accounts

The following shall be tagged as Prohibited Accounts:

a. The person has been identified by reliable sources as being a criminal or terrorist or being associated with criminal or groups;

b. The person is involved in certain criminal or such other activities that are considered to be of high risk, given the nature of the source of funds;

c. The person is from a jurisdiction which has been identified as an area/country of high risk by the financial intelligence unit and/or supervisory authority;

d. The person is from a jurisdiction identified by reliable sources as one that has high levels of criminal or terrorist activities; and

e. The employee has reason to believe, based on the behavior of the person or other factors that the transaction may be related to money laundering or the findings of terrorism.

XII. Targeted Financial Sanctions (TFS) and TFS Related to Proliferation Financing (PF)

Failure to adhere to this Manual may subject CPGI employees to disciplinary action up to the extent of termination of employment, while the contracts or business relationships with accredited third party service providers may be suspended and if necessary, termination of the contract subject to prescribed notification requirements.

Penalties for ML/TF can be severe. Under the Philippine AML Law RA 9160 as amended, a person convicted of money laundering can face up to 14 years in prison and a fine of up to P3,000,000 or twice the amount of the property involved. Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as client equity, member collateral, personal property, and, under certain conditions, entire member client accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. In addition, CPGI risk losing their charters and/or licenses, and employees risk being subjected to AML criminal investigation.

The AMLC shall, at its discretion, impose administrative sanctions upon any covered person for the violation of the AMLA and its RIRR, or for failure or refusal to comply with the orders, resolutions and other issuances of the AMLC.

Fines shall be in amounts as may be determined by the AMLC to be appropriate, which shall not be more than Five Hundred Thousand Pesos (Php500,000) per violation. In no case shall the aggregate fine exceed five percent (5%) of the asset size of the respondent.

XIII. Cooperation with the AMLC and Supervising Authorities (SAs)

Anti-money laundering laws apply not only to criminals, who try to launder their ill-gotten gains, but also to employees, who participate in those transactions, if the employees know that the property is criminally derived. “Knowledge” includes the concept of “willful blindness” and “conscious avoidance of knowledge.” Thus, employees of CPGI whose suspicions are aroused, but who then deliberately fails to make further inquiries, wishing to remain ignorant, maybe considered under the law to have the requisite “knowledge”. CPGI employees, who suspect money laundering activities should refer the matter to appropriate personnel, such as, their immediate supervisor, the designated Compliance Officer, the Group Head, and Senior Management.

PART 4: FORMS AND TEMPLATES

Annex A
Risk Assessment Form

Name of Customer:			Transaction Number:
☐ Resident ☐ Non-resident		☐ Occasional ☐ One-off	Type of occupation:
Delivery channels: ☐ face-to-face ☐ non-face to face ☐ cash-based ☐ cross border movement of cash			Purpose of Transaction:
Nature of Business/or Transaction:			
Amount:	Number of Transaction/s:		Duration/Period covered:

	MINIMUM KNOW-YOUR-CUSTOMER (KYC)/CUSTOMER DUE DILIGENCE (CDD) REQUIREMENTS:
☐	Valid ID
☐	Complete Transaction form
☐	Source of Fund declared in the form
☐	Not purporting to act on behalf of the customer. (If yes, please require authorization from the customer i.e. SPA, Sec. Cert, etc.)
☐	Customer has no Beneficial Owner (If yes, ask the client to submit a *Certification of Beneficial Owner Form)*

	Does the Customer have all the checks in the Minimum KYC/CDD Requirements?
☐	Yes. (Check if with High Risk Factor.)
☐	No. (Hold the Transaction and follow up Customer/ secure additional documents being required. After completion, check if with High Risk Factor.)

	HIGH RISK FACTORS:
☐	Source of Fund not established/ Unclear or amount involved not commensurate with the business or financial capacity of the Customer/ ID or proof of Source of Fund appears to be tampered or fake.
☐	Know-Your-Customer (KYC) document(s) or information is/are questionable/Raises doubt as to the accuracy.
☐	Warrants the filing of a Suspicious Transaction Report (STR).

	HIGH RISK FACTORS:
☐	Customer is a known Politically Exposed Person (PEP). State PEP Classification, if applicable _____.
☐	With known negative media information or suspected to be associated with convicted of an unlawful activity.
☐	Foreigner from Iran, Syria, Belarus, Burma/Myanmar, Cuba, Democratic Republic of Congo, North Korea, Somalia, Sudan and Zimbabwe (or countries in high-risk and non cooperative jurisdictions).
☐	Confirmed match in World-Check or AML Watchlist or U.N. Sanctions List.

	Does the Customer have at least one (1) High Risk Factor?
☐	Yes. (Check if EDD requirements are complete)
☐	No. Submit Transaction form.

	ENHANCEDDUEDILIGENCE(EDD)REQUIREMENTS:
☐	Submitted EDD Form.
☐	Additional documents to show proof of source of funds/income was submitted.
☐	Others _____

	Are requirements for EDD complete?
☐	Yes.
☐	No. (Hold the transaction and follow up Customer.)

Account Officer's Declaration:

I have performed the appropriate KYC process in accordance with the Anti-Money Laundering laws and policies of the Company. Should there be any adverse change in my opinion regarding the integrity or reputation of the Customer, I shall inform the Company's Compliance Officer through a Suspicious Transaction Report.

_____

Signature over Printed Name / Date

REMARKS/COMMENTS:

Reminders

A. List of Acceptable IDs:

- Passport
- Driver's License
- Professional Regulations
- Police Clearance
- Postal ID
- Voter's ID
- Photo-Bearing Barangay ID/
- GSIS e-Card
- SSS Card
- Philhealth Card
- Senior Citizen's Card
- Overseas Workers Welfare
- OFW ID
- Alien Cert. of Registration/ Immigrant Certificate of Registration
- Firearms License
- Photo bearing credit card
- Government Office ID (e.g. AFP, HDMF)
- Department of Education IDs and IDs issued by
- PRC ID
- Department of Social Welfare and Development ID/Certification Certification
- ID issued by the Bureau of Internal Revenue
- Integrated Bar of the Philippines ID
- Photo bearing health card issued by HMO
- Seaman's Book
- Photo-Bearing ID/Certification from the National Council for Welfare of Disabled Persons (NCWDP)
- Company IDs issued by private entities or institutions registered with or supervised or regulated by BSP, SEC or SA Administration ID

B. PEP is defined as:

Person who is and has been entrusted with prominent public function:

- Head of State/Head of Government
- Senior Politician – holds elected position in a city/municipal level and above
- Senior National or Local Government Officer
- Member of the Judiciary (Judges and Justices)
- Military Official (at least with a rank of Major)
- Police Official (at least with a rank of Police Chief Inspector)

PEP - refers to an individual who is or has been entrusted with prominent public position in (1) 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 PEP shall include immediate family members, and close relationships and associates that are reputedly known to have:

1. Joint beneficial ownership of a legal entity or legal arrangement with the main/principal PEP; or
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 Member of PEPs - Spouse or partner; children and their spouses; and parents and parents-in-law.
- Close Associates of PEPs – refer to persons who are 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.

C. Proof of income or source of funds should always be consistent with the Customer's declaration in the Transaction Form. Examples of documents as proof of income or source of funds include:

1. Income Tax Return
2. Payslip
3. Certificate of Employment with Salary
4. Employment Contract
5. Current Bank Statement or photocopy of Passbook
6. Bank Certificate
7. Latest Audited Financial Statement

Annex B
Enhanced Due Diligence Forms for Individual

Name of Customer: | **Transaction Number:**

Complete Current Address of Customer:

Nature of occupation/ and or business:

Source of Funds:

☐ Salary/Professional Fees/Commission ☐ Business ☐ Sale of Assets
☐ Savings ☐ Maturing Investments ☐ Insurance Proceeds
☐ Inheritance ☐ Remittance from abroad ☐ Pension
☐ Others (Please specify): _____

List of Company/ies where the Customer is a stockholder, director, officer or authorized signatory:

Name of Company/Entity	Designation

List of banks where the Customer has maintained or is maintaining an account:

Name of Bank/Entity	Maintaining Branch

Are you a Politically Exposed Person? If yes, please check the applicable box below.

☐ National and Local Government Official ☐ Head of Government Owned or Controlled Corporations
☐ Head of Foreign States ☐ Leader of Major National Political Parties
☐ Uniformed Personnel ☐ Judicial Officials
☐ Appointive Government Official (Cabinet Secretary and Undersecretary)

DECLARATION: I hereby declare under the penalties of perjury, that I have examined this form, to the best of my knowledge and belief; it is true, correct and complete. (If you are being represented by an attorney or other third party, a properly executed Special Power of Attorney authorizing the representative to act for the applicant must be included in this form).

_____
Name & Signature of Customer/Date

Annex B
Enhanced Due Diligence Forms for Legal Entity

Name of Entity: **Transaction Number:**

Complete Current Address of Entity:

List of banks where the Entity has maintained or is maintaining an account:

Name of Bank/Entity	Maintaining Branch

Details of Primary Officers (i.e. President, Treasurer, authorized signatories, etc.), directors, trustees, partners, as well as all stockholders owning five percent (5%) or more or the business or voting stock of the entity: (Please use another sheet if necessary).

Name and Nationality	Present Address	Date and Place of Birth	Nature of Work	Sources of assets

Intended nature of business relationship:

Source of Funds/Wealth (i.e. ITR, Audited Financial Statement, etc.)

Is anyone in the entity a Politically Exposed Person? If yes, please check the applicable box below.

☐ National and Local Government Official
☐ Head of Government Owned or Controlled Corporations
☐ Head of Foreign States
☐ Leader of Major National Political Parties
☐ Uniformed Personnel
☐ Judicial Officials
☐ Appointive Government Official (Cabinet Secretary and Undersecretary)

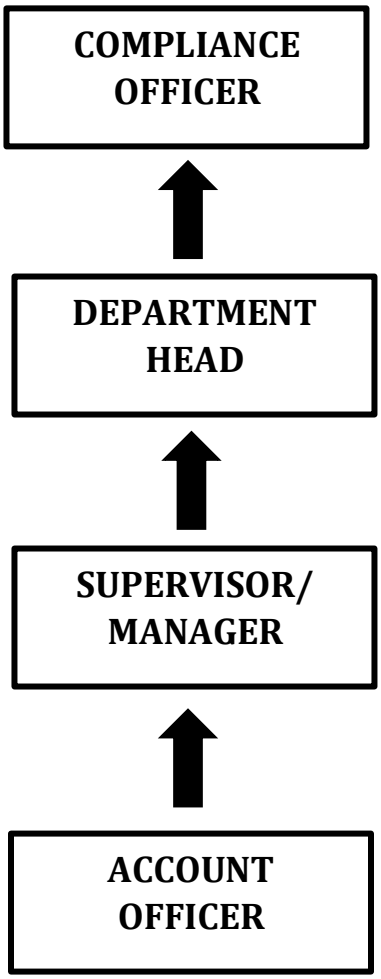
DECLARATION: I hereby declare under the penalties of perjury, that I have examined this form, to the best of my knowledge and belief; it is true, correct and complete. (If you are being represented by an attorney or other third party, a properly executed Secretary's Certificate/SPA authorizing the representative to act for the applicant must be included in this form).

_____
Name & Signature of Authorized Signatory/Date

Annex C
Comprehensive Compliance Testing Program

FREQUENCY	Annually
COVERAGE	CPGI
SCHEDULE OF TESTING	Every July
SCOPE	**I. Adoption of the MTPP** **II. Customer Due Diligence or Know-Your-Customer (KYC) Rule** a. Completeness of information obtained from customers and their representatives, if any, pursuant to AMLC regulations b. Completeness of supporting documentation obtained from individual and corporate clients c. Closure of Prohibited Accounts d. Accounts without Face-to-Face Contacts e. Beneficial Ownership f. Trust Accounts g. Effect of New Technologies h. Identification of New Products and Business Practices i. Policy Not to Transact with Clients who Fail to Provide Sufficient Evidence of Identity j. Renewal of Identification k. Cleaning out of Old Accounts l. Simplified or Reduced Customer Due Diligence m. Enhanced Customer Due Diligence n. Customer Verification 1. Accounts without Face-to Face Contacts 2. Corporate Accounts 3. Trust, Nominee and Fiduciary Accounts 4. High Risk Customers 5. Politically Exposed Persons, their Immediate Family Members and their Close Relationships/Associates o. Risk Profiling **III. Monitoring, Recording and Reporting** a. Monitoring of Transactions and Reports b. Recordkeeping c. Reporting to the Anti-Money Laundering Council **IV. Internal Control and Procedures, Compliance and Training** a. Internal Control and Procedure 1. Confidentiality Safeguards b. Executive Level Oversight c. Compliance d. Training e. Screening of Employees and Agents **V. Other Issues regarding Compliance with AML and CTF Laws, Implementing Rules and Regulations, and AMLC Issuances**

Annex D
AML/CTF Flow of Reporting of Covered and STs



Annex E
Procedure for Reporting Covered or STs

ACCOUNT OFFICER

I. For Individual customers:

1. Interview walk-in client face-to-face.
2. Require individual clients to present original and unexpired ID issued by an official authority; the ID must bear client's photo and specimen signature.

List of Valid IDs:

- Passport
- Government Office ID (e.g. AFP, HDMF)
- Driver's License
- Department of Education IDs and IDs issued by government instrumentalities
- Professional Regulations Commission (PRC) ID
- Photo-Bearing ID/Certification from the National Council for Welfare of Disabled Persons (NCWDP)
- Police Clearance
- Postal ID
- Voter's ID
- Department of Social Welfare and Development ID/Certification
- Photo-Bearing Barangay ID/ Certification
- Firearms License
- GSIS e-Card
- ID issued by the Bureau of Internal Revenue
- SSS Card
- Integrated Bar of the Philippines ID; and
- PhilHealth Card
- Company IDs issued by private entities or institutions registered with or supervised or regulated by BSP, SEC or SA
- Senior Citizen's Card
- Overseas Workers Welfare Administration ID
- Photo bearing credit card
- OFW ID
- Photo bearing health card issued by HMO
- Seaman's Book
- For Foreign Nationals**:** Passport or Alien Certificate of Registration;
- For self-employed**:** Department of Trade and Industry (DTI) Certificate of Registration and/or Business Permit issued by the local government unit.

a. In case of any doubt, double check genuineness of the ID presented by calling and confirming with the issuer of the ID.
b. Customer with false or falsified identification documents should be reported as ST.

3. In case the identification document presented does not bear any photo of the customer or authorized signatory, or the photo-bearing lD or a copy thereof does not clearly show the face of the customer or

authorized signatory, CPGI shall utilize its own technology to take the photo of the customer or authorized signatory.

4. Have the ID photocopied.
5. Sign on the photocopy to certify to the authenticity of the ID presented.
6. The Account Officer must ensure that the Transaction Form is filled out by the Client. He must also ensure that the Client confirm the details in the form before personally affixing his/her signature in the presence of the Account Officer, if applicable. The Transaction form must have the following minimum information:

    a. Name of Customer;
    b. Date and Place of birth;
    c. Name of beneficial owner (if applicable, the customer should submit a Certification of Beneficial Owners Form);
    d. Sex/Gender;
    e. Present address;
    f. Permanent address;
    g. Contact number or information;
    h. Nationality;
    i. Specimen signature or biometrics of the customer;
    j. Proof of identification and identification number;
    k. Nature of work and name of employer or nature of self-employment/ business, if applicable;
    l. Sources of funds or property; and
    m. Tax identification Number (TIN), Social Security System (SSS) number or Government Service Insurance System (GSIS) number, if applicable

7. Attach the attested photocopy to the Transaction form.
8. Do NOT accept an Transaction from a client who refuses to comply with the ID requirement.
9. File a STR regarding these cases.
10. Where the customer or authorized representative is a foreign national, the company shall require said foreign national to present valid passport, Alien Certificate of Registration, Alien Employment Permit' or any government issued identification document bearing the photograph of the customer or beneficial owner, provided that the company can be satisfied with the authenticity of the document.
11. The Account Officer will fill out the Risk Assessment Form which is a restricted and confidential form and should not be shown to the Customer.
12. If the Customer falls under the category of high risk, the Account Officer shall follow the enhanced due diligence procedure with a duly accomplished enhanced due diligence form and STR Form, if any ground exists.
13. Check the consistency of the information provided in the ID(s) presented with the minimum information in the Transaction form.
14. Submit the Risk Assessment Form together with the Transaction forms and supporting documents to Underwriting for its validation and assessment of risk. If satisfied, issue policy. Otherwise, proceed in conducting enhanced due diligence procedure.
15. Conduct on-going monitoring of customers, Accounts and Transaction/ CDD once every 2 years.

II. For corporations and other juridical entities:

1. The following information should be obtained before establishing business relationship:

a. Name of entity;
b. Name, present address, date and place of birth, nationality, nature of work and Source of Funds of the Beneficial Owner, if applicable, and authorized signatories;
c. Official address;
d. Contact number or information;
e. Nature of business;
f. Specimen signature or biometrics of the authorized signatory;
g. Verified identification of the entity as a corporation, partnership, sole proprietorship;
h. Verified identification of the entity's source of funds and business nature of the entity;
i. Verification that the entity has not been or is not in the process of being dissolved, struck-off, wound-up, terminated, placed under receivership, or undergoing liquidation;
j. Verifying with the relevant supervisory authority the status of the entity.

2. Require the corporation through its authorized representative to submit the following documents:

a. Certificates of registration issued by the Department of Trade and industry (DTl) for single proprietors; and the SEC for corporations and partnerships;
b. Secondary License or certificate of Authority issued by the supervising Authority or other government agency;
c. Articles of incorporation or association and the entity's by-laws;
d. A resolution by the ownership (board of directors or other governing body, partners, sole proprietor, etc.), authorizing the signatory to sign on behalf of the entity;
e. Latest General information sheet which lists the names of directors/ trustees/partners, principal stockholders owning at least twenty five percent (25%) of the outstanding capital stock and primary officers such as the President and Treasurer;
f. Identification documents of the owners, partners, directors, principal officers, authorized
g. Attach all the required documents to the Transaction form;
h. Do NOT submit the Transaction if the client refuses to comply with these requirements. File a STR regarding these cases; and
i. For entities registered or incorporated outside the Philippines' equivalent documents/information duly authenticated by the Philippine Consulate where said entities are registered shall be obtained.

3. For Legal arrangements Transactions and other legal entities:

a. Same information as stated in the preceding item.
b. Require the submission of the following documents:

i. list of banks where the entity has maintained or is maintaining an account;
ii. the verified name, nationality, present address, date and place of birth, nature of work, and sources of assets of the primary officers of the entity (i.e. President, Treasurer, authorized signatories, etc.), directors, trustees, partners, as well as all stockholders owning five percent (5%) or more of the business or voting stock of the entity, as the case may be;
iii. volume of assets, other information available through public databases or internet and supporting information on the intended nature of the business relationship, source of funds or source of wealth of the customer (ITR, Audited Financial statement, etc.);

iv. reasons for intended or performed Transactions; and
v. obtaining a copy of the written document evidencing the relationship between account holder or transact or and beneficial owner.

CASH MANAGEMENT AND FIELD OPERATIONS

1. Report to the company-designated AML Compliance Officer:

   a. all cash payments received that exceed P7,500,000 or its equivalent in US$ in a day.
   b. all large payments in cash, even if below P7,500,000 when, normally, this would be handled by checks.
   c. all payments using third party check or multiple checks.
   d. all payments by foreign wire transfers (regardless of amount).
   e. all payments in foreign currency coming from abroad (regardlesss of amount).

2. Incorporate these procedures in their Work Instructions and Procedures Manuals.

ACCOUNTING

1. Keep all active records originals, on microfilm or in electronic form.
2. Keep all inactive records for five (5) years from dates of termination.
3. Incorporate these procedures in their Work Instructions and Procedures Manuals.

HUMAN RESOURCES AND SALES TRAINING

1. Have adequate screening procedures when hiring employees, regardless of level, and of agents.
2. Include CPGI's anti-money laundering policy, guidelines and procedures in all orientation programs for all newly hired employees, officers and directors of the company, as well as sales agents, agency managers and branch managers.
3. As needed, schedule refresher training courses for all staff and agency force on anti-money laundering, verifying customer's identification, determining sources of funds and other related matters, inviting outside resource persons for this purpose.
4. Provide/source higher level training for the company's Compliance and Reporting Officers, Internal Auditors, Administration and Operations managers and supervisors responsible for complying with the AMLA procedures and requirements.

INTERNAL AUDIT

1. Conduct a regular audit of all affected units to ensure compliance with the Anti-Money Laundering Law, its implementing rules and regulations and this Manual.
2. Report all non-conformities as audit exceptions.
3. Conduct periodic and independent evaluation of the company's risk management, as well as the sufficiency and degree of adherence to its compliance measures. The scope shall cover the accuracy of customer identification information, CTRs/STRs, and all other records and internal controls pertaining to compliance with AML/CTF obligations.
4. Internal audits shall be conducted at such frequency as necessary, consistent with the risk assessment of the company.

DEPARTMENT HEAD

1. Report all CTs within the prescribed period.
2. If confirmed by the Compliance Officer as suspicious, report the Transaction within ten (10) calendar days of the occurrence of the Transaction, following the prescribed guidelines and procedures of the AML/CTF.
3. Maintain a complete file of all reported covered and STR forms received, even if not reported to the AMLC.

COMPLIANCE OFFICER

1. Evaluate all STRs received and determine if reasonable grounds exist. If so, have it reported by the Reporting Officer to the AMLC within ten (10) calendar days after initial detection of facts that may constitute a basis for filing such reports. If reasonable grounds do not exist, the Compliance Officer should record an opinion to that effect on the company's STR Form and return the same to the Reporting Officer.
2. All accounts received from the department where EDD was conducted must be elevated to the Board Level Committee for their approval to commence or continue business relationship.
3. Advise the management and staff on all matters relating to the prevention of money laundering.
4. Generally, ensure compliance with the provisions of the Anti-Money Laundering Law and its implementing rules and regulations.
5. Act as liaison between CPGI and the AMLC.
6. Represent CPGI in industry discussions on anti-money laundering.
7. Prepare and submit to the AMLC and SA written reports on the company's compliance with AMLA and its implementing rules and regulations.
8. Update and maintain CPGI's Manual on Anti-Money Laundering. Have the same posted on the intranet.
9. Reissue guidelines and reporting procedures as updated by the AMLC.

Annex F
Suspicious Transaction Report Form

TO: COMPLIANCE OFFICER

Transaction No.: _____

Name: _____ Transaction Date/ Period: _____

Address: _____ Transaction Amount: : _____

Name and Address of Person/s Involved (if known) : _____

Nature:

☐ Source of fund doubtful
☐ Payment by third party/ multiple checks
☐ Amount not commensurate with financial capacity/ business
☐ Payment of large sum with foreign currency (Attach Foreign Currency Form)
☐ Payment of large sum in cash No proper ID
☐ Unidentified Beneficial Owner
☐ Others (Please specify): _____

Reported by: _____ Position: _____ Contact No./ E-mail: _____

Date of Reporting: _____ Noted by (Department Head): _____

Reason/s for considering the incident suspicious:
Recommendation from Department Head:

Compliance Officer's Evaluation/ Comment:

Date Received: _____

☐ No grounds exist (state findings)
☐ For Endorsement to the Senior Management/Board of Directors
☐ Acceptance and conduct enhanced ongoing monitoring
☐ For reporting to the AMLC

_____ _____
Signature over Printed Name Date

Annex G
HR AMLA Training Plan

BACKGROUND

Aligned with the company's thrust to support the campaign against Money Laundering and Terrorism Financing, the Human Resource Services Department is submitting this AMLA Training Plan ing compliance to the AMLC's requirements.

PROPOSED PLAN AND TIMELINES

PARTICIPANTS	TYPE OF PROGRAM	FACILITATOR	TIMELINE / FREQUENCY
Directors, Management Committee Members, Division Heads and Heads of Departments and Key Departments - Finance - Marketing - Human Resources - Legal - Internal Audit - Sales - *Trainers and subject-matter- experts (SMEs) *to conduct AMLA to internal employees	Exclusive In-House or E-Learning (virtual learning) seminar with external resource.	Center for Global Best Practices	2nd week of March (one time run only)
All other officers and rank-and-file employees of CPGI. Front liners are prioritized.	In-house or E-Learning program facilitated.	CPGI's Lawyers and/or subject-matter- experts	Monthly conduct until all employees are able to attend the training and seminar.
All newly hired employees	Orientation for New Employees	HR	At least twice a month

*refresher modules to be facilitated every 2 years or as required by SA. Mode of conduct will be facilitated through E-Learning.

Annex H
Internal Audit AMLA Plan

GENERAL

The procedures described in this audit program are intended to ascertain whether CPGI is in compliance with the rules and regulations mandated by Anti Money Laundering Council per Republic Act No. 9160, as amended.

OBJECTIVE

To provide reasonable assurance that internal control system in complying Anti-Money Laundering/Combating the Financing of Terrorism (ML/CTF) regulations are followed and implemented.

SCOPE

1. Money Laundering /Terrorism Financing Prevention Program (MTPP)
2. Compliance
3. Screening and Hiring of Employees
4. Account Acceptance
5. Customer Identification and Verification
6. Account Monitoring
7. Record-Keeping
8. Reporting

PRELIMINARY ACTIVITIES

1. Review Republic Act No. 9160 as amended, AMLA Implementing Rules and Regulations, and AMLA related Circular Letters.
2. Creation of AMLA questionnaires for respective covered departments.
3. Send an audit notice to the auditee/s (Department Heads) and meet with them to discuss the purpose, objective, scope, and time table of audit.
4. Send out the questionnaires to respective department heads.
5. Conduct an assessment to the accomplished questionnaires and do a review and testing.
6. Request for additional documents, as necessary.

GENERAL GUIDELINES FOR AMLA AUDIT PROGRAM

AUDIT STEPS

PROCEDURE/CHECKLIST	YES	NO	EVIDENCE OF NON-COMPLIANCE/REF.NO.
A. Money Laundering /Terrorism Financing Prevention Program (MTPP)			
1. Check whether the company maintains a Money Laundering /Terrorism Financing Prevention Program (MTPP).			
2. Check whether the MTPP is updated, approved by the board of directors and submitted to the commission.			
3. Check whether the MTPP is complete as to the general requirements of AMLA IRR.			
4. Check whether the Board of Directors are aware of their responsibility in the approving and exercising active oversight in the implementation of MTPP.			
5. Check whether the MTPP was disseminated to all officers and staff responsible in implementing the same.			
B. Compliance			
1. Check whether the company has a designated Compliance Officer/Alternate Compliance Officer and whether he or she is aware of his or her duties.			
2. Check whether the company has compliance unit.			
3. Check the existence of record officer.			
4. Check whether the company has Customer Due Diligence measures.			
5. Check on whether the company is registered with the AMLC's electronic reporting system.			

C. Screening and Hiring of Employees			
1. Check the screening procedures when hiring employees and the corresponding verification process done.			
2. Check whether the company has continuing education, training, and refresher training program for AMLA.			
3. Check whether the education and training program covers the relevant topics as provided in AMLA IRR.			

D. Account Acceptance			
1. Check whether the company accepts anonymous accounts, accounts under fictitious names, and numbered accounts.			

E. Customer Identification and Verification			
1. Check whether the employees require customers to provide a photo-bearing ID.			
2. From the given samples, check completeness of information written in Transaction Forms for natural person: 2.1. Full name 2.2. Date of birth 2.3. Place of birth 2.4. Sex 2.5. Citizenship and nationality 2.6. Address 2.7. Contact number or information 2.8. Source of fund 2.9. Specimen signature or biometric 2.10. Name, address, date and place of birth, contact number or information, sex, and citizenship or nationality of beneficial owner, whenever applicable. 2.11. Identification documents (PhilID or other identification documents).			

3. From the given samples, check completeness of information written in Transaction Forms for juridical person: 3.1. Full name 3.2. Name of authorized representative/transactor/signer 3.3. Current office address 3.4. Contact number or information 3.5. Nature of business 3.6. Source of fund 3.7. Specimen signature or biometrics of the authorized representative/transactor/signer 3.8. Name, address, date and place of birth, contact number or information, sex and citizenship or nationality of beneficial owner, if applicable. 3.9. Certificate of Registration issued by DTI for sole proprietors, or Certificate of Incorporation or Partnership issued by SEC for corporations and partnerships, and by BSP for money changers/foreign exchange dealers and remittance agents, and by the AMLC for covered persons. 3.10. Articles of Incorporation/Partnership 3.11. Registration Data Sheet/Latest General Information Sheet Secretary's Certificate citing the pertinent portion of the Board or Partners' Resolution authorizing the signatory to sign on behalf of the entity 3.13. For entities registered outside of the Philippines, similar documents and/or information duly authenticated by 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.			

4. From the given samples, check completeness of information written in Transaction Forms for legal arrangements: 4.1. Full name of legal arrangement 4.2. Current office address and country of establishment 4.3. Contact number or information, if any 4.4. Nature, purpose and objects of the legal arrangement 4.5. 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 4.6. Deed of trust and/or other proof of existence 4.7. Other requirements for juridical persons, as applicable			

F. Account Monitoring			
1. Check whether the company conducts ongoing monitoring process.			
2. Check whether the documents collected under the Customer Due Diligence (CDD) process are kept-to-date and relevant.			
3. Check the company's process when conducting Enhanced Due Diligence (EDD).			

G. Record-Keeping			
1. Check whether the company maintains and safely store for five (5) years from the dates of Transactions all customer records and Transaction documents.			
2. Check whether the company keep all records obtained through Customer Due Diligence (CDD), account files and business correspondence, and the results of any analysis undertaken, for, at least, five (5) years following the closure of account, termination of the business or professional relationship or after the date of the occasional Transaction.			

H. Reporting			
1. Review the company's CTR and STR and check if these reports were accurately and timely reported to AMLC.			

FINAL ACTIVITIES

1. Prepare an observation memo and submit to the concerned auditee/s for matters that need clarification.
2. Reply to observation memo must be submitted within five (5) working days.
3. Consolidate the audit findings and discuss with the auditee/s for possible reconciliation.
4. Finalize the audit report.
5. Distribute the audit report to the President and Department Heads.
6. Present the audit report to the Audit Committee.
7. Conduct a monitoring on the required action items of the auditee/s, if any.

PART 5: APPROVING AUTHORITY

This version of MTPP is approved by the majority of Board of Directors, as evidenced by a sworn certification duly noted and approved by the majority of Board of Directors.

PART 6: UPDATING AND DATE OF APPROVAL

Updating

The MTPP shall be subject to the revisions and/or new implementing rules. As such, this Manual will be updated accordingly.

The MTPP shall be regularly updated at least once every two (2) years to incorporate changes in the AML policies and procedures, latest trends in ML/TF typologies, and latest pertinent SA and/or AMLC issuances.

In case of revisions, the Compliance Officer shall submit to the SA not later that fifteen (15) days from the approval of the majority of Board of Directors of the new/updated MTPP, a sworn certification that a new/updated MTPP has been prepared, duly noted and approved by the majority of Board of Directors.

Date of Approval

This version of MTPP is approved by the Board of Directors on July 14, 2022.

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

SWORN CERTIFICATION

I, **DANNY E. BUNYI**, Filipino, of legal age, duly elected Corporate Secretary of CENTURY PROPERTIES GROUP, INC. (the "Corporation"), a corporation duly organized and existing under the laws of the Republic of the Philippines with principal office address at the 8/F Pacific Star Bldg. Se. Gil Puyat cor. Makati Avenue, Makati City, Philippines, after having been duly swron in accordance with law, despose and state that:

That the Board of Directors duly noted and approved the Money Laundering and TerrorismFinancing Prevention Program (MTPP) on July 14, 2022.

IN WITNESS WHEREOF, I have hereunto signed this Certificate this JUL 14 2022 2022 at MAKATI CIT City.

DANNY E. BUNYI
Corporate Secretary

SUBSCRIBED AND SWORN to before me this _____ day of JUL 14 2022 2022. The affiant exhibited to me his Driver's License N02-86-041246 valid until 2026/08/08.

Doc. No. 398.
Page No. 81.
Book No. II.
Series of 2022.

NOTARY PUBLIC

DIN-DIN A. CRUZ
Appointment No. M-007
Notary Public for Makati City
Until December 31, 2023
23rd Floor, Century Diamond Tower, Century City,
Kalayaan Avenue corner Salamanca Street,
Barangay Poblacion, Makati City
MCLE Compliance No. VII - 0000259, 07.30.2019
PTR No. MKT 8853292MJ, 01.03.2022 / Makati City
Roll No. 55143 / IBP No. 172081, 01.05.2022 / Makati City