PROPEL GLOBAL BERHAD

Registration No. 202001023868 (1380188-P)

ANTI-MONEY LAUNDERING AND COUNTER FINANCING OF TERRORISM (AML/CFT) POLICY

Reference No.	SER_PO002
Version	1.0
Effective Date	22 February 2023
Document Owner	Corporate Office/ Group Compliance Officer

DOCUMENT CHANGE HISTORY

Version	Date	Summary of Changes	Approved By
1.0	22.02.2023	New document	BOD of PGB

CAUTION

The details described in this document are not exhaustive to the extent of excluding the personnel from exercising good judgement and discretion

However, all personnel must always bear in mind that the underlying principle is to always safeguard the company' interest and to avoid occurrence of any financial loss and/or incidences which could adversely impact the company's good name and image

TABLE OF CONTENTS

GLOSSARY

No	Terms	Description
1	AC	Audit Committee
2	AML/CFT	Anti-Money Laundering & Counter Financing of Terrorism
3	AMLATFA	Anti-Money Laundering and Anti-Terrorism Financing Act 2001
4	BL	Business Lead
5	BOD	Board of Directors of PGB
6	CDD	Customer Due Diligence
7	CMSA	Capital Markets and Services Act
8	Counterparty	Business relationship with PGB i.e., buyer, supplier, contractor, sub-contractor, consultant, outsource party
9	Customer	Defined as counterparty having a business relationship with PGB
10	FATF	Financial Action Task Force – International body handling/regulates Anti Money Laundering and Counter Financing Terrorism
11	FIED	Financial Intelligence and Enforcement Department – Bank Negara Malaysia department handling all matters on Anti Money Laundering and Counter Financing of Terrorism
12	GCEO	Group Chief Executive Officer
13	HR	Human Resources
14	HLC	Head of Legal & Compliance
15	HOD	Head of Department
16	ISTR	Internal Suspicious Transaction Report
17	Management	Management of PGB, which includes GCEO, CFO and BL
18	ML/TF	Money Laundering/Terrorism Financing
19	OFAC	The Office of Foreign Assets Control a US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy countries and regimes, terrorist, international narcotics traffickers, those engaged in activities related to proliferation of weapon of destruction, and other threats to the national security, foreign policy or economy of the United States

20	PGB	Propel Global Berhad
21	SAR	Suspicious Activity Report
22	SC	Securities Commission Malaysia
23	STR	Suspicious Transaction Report
24	UN LIST	United Nation Security Counsel List
25	US OFAC	US Office of Foreign Assets Control

End of Section

1. INTRODUCTION

1.1 Background

Money laundering and terrorism financing (ML/TF) continues to be an on-going threat which has the potential to adversely affect the country's reputation and investment climate, which may lead to economic and social consequences. The globalisation of the financial services industry and advancement in technology has posed challenges to the regulators and law enforcement agencies as criminals have become more sophisticated in utilising financial institutions/non-financial platform to launder illicit funds and us them as conduits for ML/TF activities.

While SC has been putting in vigorous efforts in building the AML/CFT compliance framework for all reporting institutions to address the ML/TF risks and vulnerabilities, continuous effort is in place to access the effectiveness of our AML/CFT framework to ensure that it continues to evolve in line with developments in international standards and the global environment.

1.2 Objectives

1.2.1 To provide basic policy to follow as well as to highlight the regulatory requirements for all staff of PGB in conducting their business in conformity with high ethical standards and be on guard against undertaking any business transaction that is or may relate to or may facilitate ML/TF.

1.3 Scope and Applicability

1.3.1 The scope of this policy is inclusive of all business transactions handled by PGB.

1.3.2 This policy applies to PGB holding and all its subsidiaries.

1.3.3 This policy applies to all employees of PGB Group.

1.4 Approval and Exception

1.4.1 This policy and changes here forth shall be approved by the BOD / Delegated Board Committee.

1.4.2 Although PGB may not be classified as a Reporting Institution under the AMLA Act, however, all companies and everyone is subject to AMLA laws if an act of ML/TF is suspected in which may cause reputational risk to the company.

1.5 Regulatory Requirements

1.5.1 This policy is intended to comply with the following or any available Act that relates to countries that PGB or its subsidiaries operate:

- Corporate Code of Conduct & Ethics
- Related Party Policy

- Personal Data Protection Policy
- Anti-Bribery and Corruption Policy
- Anti-Money Laundering Policy
- Records Management Policy
- Anti-Money Laundering and Anti-Terrorism Financing Act 2001
- Securities Commission Act 1993
- Guidelines on Prevention of Money Laundering and Terrorism Financing for Reporting Institutions in Capital Market issued by Securities Commission (SC)

1.5.2 This policy must be read in conjunction with (not exhaustive):

- Circulars issued as and when that has relevance to this document

1.6 Definitions

Terms	Descriptions
Beneficial Owner	Means the natural person(s) who ultimately owns or controls a customer and / or the natural person on whose behalf a transaction is being conducted. It also includes that person who exercises ultimate effective control over a legal person or arrangement. Reference to 'ultimately owns or controls' and 'ultimate effective control' refers to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.
Money Laundering	Is the process of converting money/property, which is derived from illegal activities to give a legitimate appearance'.
PEP (Politically Exposed Person)	(a) Foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials; (b) Domestic PEPs – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or Government, senior politicians, senior government, judiciary or military officials, senior executives of

Terms	Descriptions
	state-owned corporations and important political party officials; or (c) Persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the BOD or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.
Reputational Risk	Reputational risk is the risk of current and prospective impact on earnings and capital arising from negative public opinion. Such risks affect PGB's ability to establish new relationships or services or continue servicing existing relationships. Reputation risk may expose PGB to litigation, financial loss or a decline in PGB's customer base. It is recognised that if not addressed, may result in negative impacts such as unavailability of services, information deficiencies, financial losses, increased costs and importantly, the ***loss of reputation.*** As such, PGB is desirous to manage this risk indirectly.
Terrorism Financing	Generally, terrorism financing (TF) refers to carrying our transactions involving funds that may or may not be owned by terrorist, or that have been, or are intended to be, used to assist the commission of terrorism.
Counter Party	Refers to any customer of PGB such supplier, contract party, consultant, buyer o**r** any party that PGB has dealings with where payment are made to or receipt of funds from.
Sanctions	There are individual/countries where United Nations Security Council (UNSC) has taken measures to sanction the individual or country to counter terrorism. Sanctions list can be obtained from UN list at: https://www.un.org/securitycouncil/content/un-sc-consolidated-list

2. PRINCIPLES

End of Section

3. POLICY STATEMENTS

3.1 Principle 1 – Guidelines on AML/CFT Requirements

3.1.1 It is vital for all employees to understand the basic understanding of money laundering. The three stages of money laundering are known as:

- Placement

  The physical disposal of proceed derived from illegal activities

- Layering

Separating the illicit proceeds from their sources through transactions that disguise the audit trail and provide anonymity

- Integration

  Integrating the laundered proceeds into the economy as normal funds

3.1.2 Section 3(1) of AMLATFA defines money laundering as act of a person who:

- Engages, directly or indirectly in a transaction that involves proceeds of any unlawful activity

- Acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from, or brings into Malaysia proceeds of any unlawful activity; or

- Conceals, disguises or impeded the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceeds of any unlawful activity:

  Where:

  - As may be inferred from objective factual circumstances, the person knows or has reason to believe, that the property is proceed from any unlawful activity; or

  - In respect of the conduct of a natural person, the person without reasonable excuse fails to take reasonable steps to ascertain whether the property is the proceeds from any unlawful activity.

3.1.3 Section 3(1) of AMLATFA defines the financing of terrorism offence which include:

- Providing or collecting property for carrying out an act of terrorism

- Providing services for terrorism purposes

- Arranging for retention of control of terrorist property

- Dealing with terrorist property

3.1.4 Conducting Due Diligence on counterparty

- PGB employees must conduct appropriate due diligence to understand the business and background of PGB prospective business counterparty and to determine the origin and destination of money, property, and services.

3.2 Principle 2 – Sanction Individual/Countries of counterparty

3.2.1 UNSC Sanction List

- PGB to download and keep the sanction list for counterparty checking. Such list must be kept updated by keeping abreast of world affairs to update the list.
- Counterparty checking must be performed against the list avoiding seizure of properties or funds when remitting or receiving funds from if sanction individual or country.

3.2.2 The Office of Foreign Assets Control (OFAC) Sanction List

- In dealing with US dollars, the OFAC sanctions list must also be kept avoiding any payments or receipt of funds remitted in US dollars being confiscated due to sanction by United States of America's Treasury.

3.2.3 Name matches in Sanction List

- For name of counterparty matches, further Enhanced Due Diligence check is required based on risk-based approach to investigate the particulars of the counterparty thoroughly as such requiring more evidence and detailed information on the reputation and history to be collected.
- Once confirmation has been obtained, PGB must immediately:
    - Reject the potential counterparty;
    - Block the transaction, where applicable;
    - Submit suspicious transaction report; and
    - Inform the relevant supervisory authorities.

3.3 Principle 3 – ML/TF Risk Profiling on Counterparty

3.3.1 Risk Assessment

- Appropriate steps must be taken to identify, assess and understand its ML/TF risks in relation to its counterparty, countries or geographical areas and products, services, transactions or delivery channels.
- Procedures must be in place for assessing ML/TF risks on counterparty:
    i. Documenting their risk assessments and findings;

ii. Considering all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
iii. Keeping the assessment up to date through a periodic review; and
iv. Having appropriate mechanisms to provide risk assessment information to the supervisory authority.

- Additional assessment when requested by the supervisory authority.

3.3.2 Risk Profiling

- Risk profiling must be conducted on counterparty with considerations of following factors:

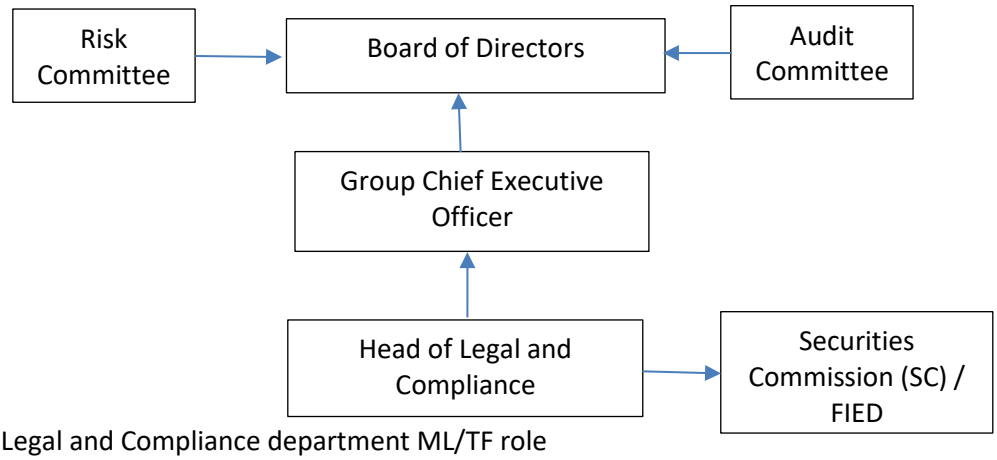
i. Counterparty risk (e.g. resident or non-resident, type of customers, occasional or one-off, legal person structure, types of PEP, types of occupation);
ii. Geographical location of business or country of origin of counterparty;
iii. Products, services, transactions or delivery channels (e.g. cash-based, face-to-face or non-face-to-face, cross border); and
iv. Any other information suggesting that the customer is of higher risk.

- PGB is required to regularly review and update the counterparty risk profile based on their level of ML/TF risks.

- The relevant department/business unit engaging in risk assessments and profiling must provide timely reporting of the risk assessment, ML/TF risk profile and the effectiveness of risk control and mitigation measures to the Risk Committee or any Delegated Board Committee.

3.4 Principle 4 – AML/CTF Compliance Structure in the Organization

3.4.1 For the AML/CFT Compliance Program to be effective, PGB is to establish a clear reporting structure/line



3.4.2 Legal and Compliance department ML/TF role

- Legal and Compliance department must ensure internal programs on AML/CFT are adhered to including proper maintenance of records and reporting of suspicious transactions.

3.4.3 Employee Training and Awareness Program

- Ensure that awareness and training program on AML/CFT practices and measures are conducted for employees, in particular 'frontline' staff and officers in charge of processing and accepting new counterparty as well as staff responsible to monitor transactions.

- Training for all employees may provide a general background on ML/TF, the requirements and obligations to monitor and report suspicious transactions to the Compliance Officer and the importance of conducting CDD.

- Employees must be aware that they may be held personally liable for any failure to observe the AML/CFT requirements.

- These training and awareness programs should be conducted regularly and supplemented with refresher courses for employees and staff must be updated on the latest AML/CFT developments such as products or transaction modes which are susceptible to the risk of money laundering and financing of terrorism.

- Compliance Officer is responsible for staff training records.

3.5 Principle 5 - Customer/Counterparty due diligence ("CDD") requirements

3.5.1 Customer identification must be verified

- Customer identification must be verified against a reliable source.

- Take reasonable measures to understand the control of the account and the beneficial owner of the account, using the relevant information or data obtained from a reliable source to be reasonably satisfied that it knows who the beneficial owner is.

- Identify the source or destination of funds (where applicable).

- Unwillingness of customer/counterparty to provide information requested for CDD shall be a factor for suspicion.

- Business relation should not be commenced for new counterparty or to be terminated for existing counterparty, if fails to comply CDD.

- In certain circumstances where the ML/TF risks are assessed as low and verification is not possible at the point of establishing the business relationship, PGB may complete verification after the establishment of the business relationship to allow some flexibilities for its counterparty and beneficial owner to furnish the relevant documents.

- Where delayed verification applies, the following conditions must be satisfied:

  i. This occurs as soon as reasonably practicable i.e., refers to time frame not later than ten working days or any period as specified by SC;
  ii. The delay is essential so as not to interrupt PGB normal conduct of business;

iii. The ML/TF risks are effectively managed; and
iv. There is no suspicion of ML/TF risks.

- Notwithstanding the above requirements, the following categories are exempted from obtaining constituent document, and from identifying and verifying the directors and shareholders of legal persons:

i. Public listed companies/corporation listed in Bursa Malaysia or majority owned subsidiaries of such public-listed companies.
ii. Foreign public-listed companies recognized by Bursa Malaysia and not listed in the jurisdiction identified in the FATF Public statements.
iii. An authorized person, an operator of a designated payment system, a registered person under Financial Services Act 2013 or the Islamic Financial Services Act 2013.
iv. Entities licensed under the Labuan Financial Services and Securities Act 2010 or Labuan Islamic Financial Services and Securities Act 2013.
v. Prescribed Institutions under the Development Financial Institutions Act 2002.

3.5.2 Ongoing due diligence Monitoring

- Scrutinising transactions undertaken throughout the course of the relationship to ensure that the transactions being conducted are consistent with PGB knowledge of the customer/counterparty, risk profile and source of funds.

- Ensure that documents, data and information collected under the CDD proceed is kept up to date and relevant, by undertaking reviews for higher risk customers.

3.6 Principle 6 - Politically Exposed Person ("PEP")

3.6.1 Family member s and close associates of the PEP

- The requirements set out here are applicable to family members (i.e., spouse, parent, sibling, or children) or close associates/advisor of all types of PEPs. Special attention is required if it is known that a particular business/company is owned by personal mentioned above, then the business/company account is deemed to be PEP too. This stringent observation is necessary as the related business and personal involve reputational risks like those with PEP themselves.

3.6.2 Possibility of PEP abuse of their public powers

- All staff are to be aware of the risks involved in dealing with PEPs lies with the possibility of such PEPs abusing their public powers for their own illicit enrichment, especially in countries where corruption is widespread/known in the international market.

3.6.3 Reputational Risk in relations with foreign PEPS

- Relations with foreign PEPs may expose PGB to significant reputational and/or legal/regulatory risks. There is always a possibility that PGB may be implicated, when

there is an established relationship, if such persons abuse their public powers for their own illicit enrichment through the receipt of bribes, embezzlement, misuse of public assets etc.

3.7 Principle 7 – Suspicious Transaction

3.7.1 What are the considerations that constitutes as Suspicious Transaction?

- The unusual nature or circumstances surrounding the transaction.
- The known business of the person conducting the transaction does not reflect the nature of the business according to the knowledge of PGB.
- False identification in connection with the transaction, different addresses, multiple contact numbers, etc.
- The behaviors of the person conducting the transaction.
- Inability to complete CDD.
- Unreasonably evasive or uncooperative.
- Appears illegal and indicate that the customer is involved in ML/TF.

3.7.2 Notice of Suspicious Transaction

- Must be conducted in a secured environment to maintain confidentiality and preservation of secrecy.
- All staff of PGB must know the reporting procedures for suspicious transaction reporting.
- Failure to report if reasonable grounds to believe that the transaction is "suspicious" is an offence under the AMLA.

3.7.3 Tipping Off

- Once the suspicious transaction reporting has commenced, all staff including directors should not:

  i. Warn/Tip-off the person(s) who is the subject of the suspicious activity report;
  ii. Notify any other persons in PGB (only on need to know basis); or
  iii. Notify any other person outside PGB.

- AMLA Section 24 provides protection on disclosure of information/secrecy imposed by any written law, if they report their suspicion in good faith to the regulator or relevant enforcement authorities.
- All staff are to comply with the request should law enforcement agencies request for information.

3.8 Principle 8 - Records and documents pertaining to AML/CFT

3.8.1 Records and documents retention

- Records and documents pertaining to money laundering/terrorist financing shall be maintained for at least seven (7) years from the date an account has been closed or relationship has been terminated or completed.
- Where the records are subject to ongoing investigations or prosecution, all relevant records must be kept beyond the stipulated retention period until SC or the enforcement agency confirms that those records are no longer required.
- Types of records to be retained for the purpose of AML/CFT are:
    - Customer profiles, including customer transaction forms, documents used to verify the identity of customers and beneficial owners, and result of any analysis undertaken.
    - Transaction records and supporting documentations.
    - Suspicious Activity Reports and Suspicious Transaction Reports with supporting documentation.
    - All Money Laundering/Terrorism Financing investigation files.
    - Records of all formal Anti-Money Laundering/Counter Financing of Terrorism training conducted which include the names, business units of attendees, dates and locations of the training.
    - Any other documents required to be retained under applicable Money Laundering/Terrorism Financing law.
- Clear Audit Trails of the records must be kept for easy traceability by the relevant authority and law enforcement agencies.

3.9 Principle 9 - Know Your Customer/Counterparty

3.9.1 The KYC procedure

- KYC procedure enables companies to identify and verify the identity of a customer and to ensure that the customer is actually who they say they are. As part of Due Diligence, the aim of the KYC check is to prevent business relationships from being established with persons who are associated with terrorism, corruption, or money laundering, among other things
- Minimum information that a company must have on their counterparty
    - Name of the person conducting the transaction
    - Identification of the Individual / company

- Source of funds / Purpose of funds
- Contact details
- Acceptance / permission to allow personal data to be collected for various purposes in the course of registering / processing the application.

End of Section

4. ROLES AND RESPONSIBILITIES

Roles	Responsibilities
Board / Delegated Committee	➢ Deliberate and approve the policy ➢ Adequate oversight of the overall AML/CFT measures ➢ Committed in establishing an effective internal control system for AML/CFT
Audit Committee	➢ Review internal controls and issues identified on AML/CFT program ➢ Ensure that independent audits are conducted
Risk Committee	➢ Ensure adequacy of the policy and procedure in identifying, measuring, monitoring and controlling risks relating to AML/CFT ➢ Ensure periodic reports on risk exposure (if any) and risk management ➢ Ensure compliance with prevailing guidelines on AML/CFT
GCEO	➢ Ensure BOD is updated with timely information on the AML/CFT risk ➢ Ensure procedures are formulated on AML/CFT ➢ Aware of the risk associated with ML/FT
Legal and Compliance Department	➢ Overall responsible on AML/CFT program including keeping abreast on prevailing guidelines on AML/CFT
All Staff	➢ Awareness on AML/CFT ➢ Adherence to the AML/CFT policy
Financial Intelligence and Enforcement Department (FIED)	➢ Bank Negara Malaysia department handles all matters on AML/CFT including the investigation on Suspicious Transaction Reporting
Securities Commission (SC)	➢ Handles matters on AML/CFT for companies in the Capital Markets

---------- END ----------