ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM (AML/CTF) POLICY

ABBREVIATIONS

Abbreviation	Description
AML	Anti-money laundering
CDD	Client due diligence
CIP	Client identification procedures
CKYCR	Central KYC Records Registry
CTF	Countering Terrorist Financing
EU	European union
FATF	Financial action task force
FCC	Financial crime compliance
PPATK	The Indonesian Financial transaction Reports and Analysis Centre (PPATK) Pusat Pelaporan dan Analisis Transaksi Keuangan
GRC	Global Risk Compliance
KYC	Know your customer
NGO	Non-governmental organization
NSDL	National securities depository limited
ML/TF	Money laundering and terrorist financing
OFAC	Office of foreign assets control
OVD	Officially Valid Document
PEP	Politically Exposed Persons
SAR	Suspicious activity report
STR	Suspicious transaction report
UBO	Ultimate Beneficial Owner
UN	United Nations

DEFINITIONS

a. "**AML Policy**" means this document, that is, anti-money laundering policy/ combating the financing of terrorism, as approved and adopted by the Board of PT Asianet Media Teknologi.

b. "**Board**" means the board of directors of PT Asianet Media Teknologi.

c. "**Business Partner**" means all entities and individuals who supply products, equipment, materials or provide services to PT Asianet Media Teknologi under a contract, agreement or arrangement, it also includes agents, sub-contractors and representatives/employees of such Business Partner.

d. "**Client**" means Business partners, delivery partners and Merchants cumulatively.

e. "**Employee(s)**" includes all definite and indefinite employees whether referred as staff, worker, consultant, retainer, personnel or by any other equivalent/similar term of PT Asianet Media Teknologi.

f. "**Master Directions**" means the Master Direction – Know Your Customer (KYC) Direction, 2016, and guidelines on regulation of payment and payment gateways as updated or amended from time to time.

g. "**Merchant**" means all the partners who are live on PT Asianet Media Teknologi platform or availing services.

h. "**Officially Valid Document**" or "**OVD**" means any identity document issued by the government of *Republic of Indonesia* containing name, address and photo of the person. For example, Kartu Tanda Penduduk (KTP), passport, and driving licence.

i. "**Politically Exposed Persons**" or "**PEP(s)**" means individuals who are or have been entrusted with prominent public functions in a foreign country, e.g., heads of states/governments, senior politicians, senior government/ judicial/ military officers, senior executives of state-owned corporations, important political party officials, etc.

j. "**Principal Officer**" means an officer nominated by the Board who will be responsible for creating, implementing and maintaining whole AML framework in the Company.

k. "**Sanctions Exposure**": Any Customer having direct or indirect connection to any of the sanctioned countries or individuals as per OFAC, UN and EU.

l. "**Ultimate Beneficial Owners**" or "**UBO**":

An individual who may appoint or dismiss directors, board of commissioners, management, or supervisors of the corporation; possess the authority to control the corporation; entitled to receive, and/or receives benefits directly or indirectly of the corporation; is the true owner of the corporation's fund or shares and/or fulfils the criteria of a beneficial owner under the Presidential Regulation. Under the Presidential Regulation, every corporation must determine at least 1 (one) BO of the corporation in accordance with the criteria:

a. holds shares of more than 25% of a limited liability Company as stated in the articles of association;
b. has a voting rights of more than 25% of a limited liability Company as stated in the articles of association;
c. receives profit of more than 25% of the profit earned by a limited liability Company per year;
d. has the authority to appoint, displace, of dismiss members of the board of directors and members of the board of commissioners;
e. has the authority or power to influence or control a limited liability Company without having to obtain any authorization from any parties;
f. receives benefits from a limited liability Company, and/or;
g. is the true owner of the funds of the ownership of shares of a limited liability Company.

The term "*control*" includes the right to appoint majority of the directors or to control the management or policy decisions exercisable by a person or persons acting individually or in concert, directly or indirectly, including by virtue of their shareholding or management rights or shareholders agreements or voting agreements or in any other manner.

The term "*significant influence*" is defined as the power to participate, directly or indirectly, in the financial and operating policy decisions of a Company but does not include control or joint control of those policies.

1. OBJECTIVE AND APPLICABILITY

This AML Policy outlines the internal guidelines to be followed by PT Asianet Media Teknologi and are aimed to implement the Anti-Money Laundering and Countering Terrorist Financing (AML/CTF) principles. This AML Policy is applicable mutatis mutandis to all types of businesses conducted by the Company and are also intended to be applicable to any future businesses which the Company may engage in, with necessary modifications, as applicable. This policy is also applicable to all the branches, employees, business partners and business correspondents (BCs)/ agents who represent or provide or avail any service by/to the Company PT Asianet Media Teknologi.

Failure to comply with this AML Policy by any Employee, both in letter or in spirit, or an attempt to circumvent this directly or indirectly, may lead to disciplinary action leading up to and including dismissal and such Employee may be reported to the relevant regulatory authorities, which might lead to criminal proceedings.

2. SCOPE

- AML Policy covers the provisions for the following AML areas:
    - Client acceptance
    - Client due diligence (CDD)
        i. KYC documentation and verification
        ii. Name screening
    - KYC refresh / re-KYC
    - Rejecting/terminating business relationship
    - Escalation and management reporting
    - Record keeping
    - Designated officers
    - Regulatory reporting
    - Training
- AML Policy is for the platform aggregation (PA) business of PT Asianet Media Teknologi. As of 14 January 2019, PT Asianet Media Teknologi operates in Indonesia.
- A robust governance structure shall be implemented to monitor compliance with AML, KYC and CTF guidelines defined in this document, across all functions / business units of the Company. The Compliance Committee will oversee the implementation of the AML/ CTF framework.
- A senior management officer shall be appointed as the Principal Officer who will facilitate and monitor compliance with regulatory guidelines as applicable to the Company with respect to client acceptance, client due diligence, reporting and risk management.
- This AML Policy shall be reviewed by the Compliance team on annual basis. Amendments, if any, shall be done by Principal Officer and put before the Board for their approval.

3. REGULATORY OVERVIEW

Below is the AML regulatory snapshot *of Indonesia* which may be indirectly applicable to the Company.

Indonesia - The Act 8 of 2010 regarding Prevention and Eradication of Money Laundering Act regulates individual or corporation who is inside or outside Indonesian territorial that attempt or conduct or assist to commit money laundering act will be punished under the Act 8 of 2010. Best practices guidance suggests that should consider adopting a robust risk-based AML/CTF program which outline all of the functions of effective monitoring and should safeguard the Company from ML/TF regulatory, legal fines, and reputational damage.

4. CLIENT ACCEPTANCE

The Company shall perform checks with regards to the line of business and industry before on-boarding a client and might not on-board the clients who are dealing in illegal activities[1], like drugs, pornography, hawala, human trafficking, terrorism or any other illegal activities/business as per Indonesian law. Also,the Company might not accept a client, if the client is:

- having anonymous or fictitious/benami name;
- not willing to furnish the documents/information required to complete KYC;
- in any sanctions watchlist;
- in internal blacklist; or
- having intentions to exploit product for money laundering/Terrorist financing (ML/TF) purposes.

The Company might accept the individuals/entities enlisted below as Client:

- Resident individuals;
- Companies / body corporate with registered office in Indonesia;
- Partnership firms;
- Sole Proprietorship firms;
- State- Owned Enterpries (Badan Usaha Milik Negara)
- Limited Liability Partnership (LLP) firms;
- Private Limited firms;
- Public Limited firms; and
- Trusts, foundations, NGOs, Charitable Bodies.

5. CLIENT DUE DILIGENCE

Due diligence stage is an integral part of any AML process, where the On-boarding Team of the Company collects KYC documents and verifies the identity of client, as well as its ultimate beneficial owners and authorised signatory, in case of an entity.

6. 6a. KYC DOCUMENTATION AND VERIFICATION

Onboarding Team shall collect the following KYC documents from client at the time of onboarding digitally or in physical form, for the purpose of identification. The Company shall apply below KYC documentation guidelines on existing clients in a phased manner.

Business Partners

- In case of Individual/Sole Proprietorship – Kartu Tanda Penduduk (KTP) or equivalent registration proof, proof of address, photo, proof of bank account
- In case of other entity types – Proof of nature of business, registration proof, proof for registration address, proof/declaration for authorized signatory and beneficial owner names, KTP of authorized signatory and beneficial owners.

6b. SCREENING

Based on Act 8 of 2010 regarding Prevention and Eradication of Money Laundering, Principal Officer shall ensure that at the time of on boarding the Company screens its business partners, having Rp100 Million or more business with the Company in a fiscal year, against applicable watchlist. These watchlist include the sanctions list of entities and individual issued by the Office of Foreign Assets Control (OFAC), UNSC watchlist and EU watchlist circulated by Bank of Indonesia, along with other blacklists.

[1] Illegal activities may include drugs, pornography, hawala, human trafficking, terrorism activity or any other illegal activities/business as per the prevailing laws

The Company shall apply the screening guidelines on existing merchants and business partners in a phased manner.

If sanctions screening returns a positive match the Company will reject or terminate the Customer relationship or if there are any doubts as to the result of sanctions screening, cases should immediately be referred to the Principal Officer for further advice.

7. PERIODIC CDD

Once in every year, an implicit notification shall be sent to business partners seeking information on any change in demographic details, otherwise existing record will be considered as updated one.

If there is any change in demographic information received from business partners, following are the steps to be followed:

KYC verification

Collect the proof for updated KYC information and ensure that it is verified using reliable sources and correctly maintained in the internal systems.

Screening

The on-boarding team shall check change in client's name,the names of their beneficial owners and any other authorised signatories against the watchlists.

8. REJECTING/ TERMINATING THE BUSINESS RELATIONSHIPS

Client relationship may be rejected if there is a suspicion that the aim of establishing the relationship was ML/TF. A client relationship may be rejected or terminated on the occurrence of the following events, including but not limited to:

- Where CDD measures are not possible to be performed on a Client.
- Positive hit against applicable Sanctions watchlist.
- Where documentation or identity is identified as potentially counterfeit or forged.
- Where a Client is identified as being directly or indirectly associated with terrorists or terrorist activity.
- Where a Client is identified as directly or indirectly involved in corruption, crime or tax evasion.

The reason and the rationale for declining or terminating the business relationship shall be recorded.

All exit decisions taken by Onboarding,Risk Compliance, Supply Chain Management, Finance, or Corporate Secretary shall be notified to the Principal Officer along with the detailed rationale and media screening reports.

In instances where a relationship is being exited because of ML/TF or sanctions suspicions, the Risk Compliance team along with Principal Officer should consider informing the relevant authorities via a Suspicious Transaction Report (STR).

9. ESCALATING AND REPORTING TO SENIOR

Any findings made during the execution of the CDD process, which raise suspicion or give reasonable grounds to suspect that the Company may be intended to be used as a medium for offences related to ML/TF, shall be escalated to Principal Officer.

In the event of rejecting/terminating any Client's relationship, the Risk Compliance team will escalate all cases to the Principal Officer for approval.

10. RECORD KEEPING

The Company shall maintain the information and documentation relating to KYC of client. All documents obtained for KYC/CDD purposes, such as Company documents, identity documents and application forms shall be stored digitally or in physical files, during the course of business relationship and for at least 10 years from the date of cessation of the relationship with the client.

The Company shall also maintain the KYC/CDD documents of the clients for at least 5 years, who have been rejected from onboarding or terminated based on ML/TF suspicion and STR has been filed with relevant authority.

The Company shall ensure that all KYC/CDD information is readily available, easily accessible and retrievable in a timely manner, during inquiry received from the competent authorities.

11. PRINCIPAL OFFICER

The Board of the Company shall nominate a 'Principal Officer', who will be responsible for managing and ensuring AML/CTF compliance, monitoring transactions, and sharing and reporting information. Detailed responsibilities of Principal Officer are:

- Ensure dissemination of KYC and AML/CTF updates to business units and guide them on compliance;
- Identify emerging areas of risks of non-compliance with KYC and AML/CTF guidelines;
- Ensure that all suspicious activities of clients are reported in an accurate and timely manner and
- Review and approve the AML/CTF training modules for relevant employees.

The Principal Officer must have the ability to communicate effectively, in both ritten and verbal format, at all levels of the organization – from front line associates to all the way up to the CEO and Board.

12. REGULATORY REPORTING

Although there is no direct reporting obligation on the Company, however, if any suspicious activity is noticed for a Client, the transaction settlement should be suspended related to that particular client, and Suspicious Transaction Report (STR) should be filed with PPATK. Principal Officer & Risk Compliance department on being satisfied that the transaction is suspicious, shall have the same reported within 7 working days to PPATK. In the case of transactions involving frauds, the Company shall also inform the relevant police units and other (law enforcement) units. Further, the assets on the account shall be frozen in case client has Sanctions exposure.

The company will keep a register of suspicious transactions related to its businesses and shall not inform any client or any other unauthorised persons that a transaction has been reported as a suspicious transaction.

The Company shall block funds and transactions whenever:

- A transaction is deemed suspicious;
- Client is having a positive Sanctions match or has Sanctions exposure; or
- A request to block client's fund is made by any regulatory body or law enforcement agency.

13. TRAINING

Employees play an important role for an effective AML program. Hence, employees of Risk Compliance, onboarding team, Finance (Pay-out) team, Legal team and senior management shall be trained appropriately on the relevant ML/TF legislations, risks and mitigation methodologies. The Company shall ensure that AML related training is provided to all relevant employees (old/ new) via third party online platform expert in disseminating AML trainings.

The Company shall implement online training related to AML, KYC and sanctions compliance, and Principal Officer will be responsible to conduct these trainings and keep course up to date.