AML	Anti-Money Laundering
WPM	WPM INTERNATIONAL, LLC.
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
CIBO	Client Identification and Beneficial
FT	Ownership Financing of Terrorism
ID	Identification
KYC	Know Your Customer
ML	Money Laundering
VR	Verification

1. WPM INTERNATIONAL, LLC. - COMMITMENT

1.1 WPM will follow all relevant U.S. guidelines for combating Money Laundering and the Financing of Terrorism by implementing internal measures as may be deemed necessary.

2. POLICY CUSTODIAN

2.1 The WPM Management Team will be responsible for the implementation and enforcement of company policy.

2.2 The WPM Management Team will seek the support of law enforcement and/or other government entities when necessary in order to utilize their expertise and assistance regarding the implementation and enforcement of our policies.

3. PURPOSE AND RATIONALE

3.1 This policy sets out provisions, procedures and controls as enacted by WPM concerning Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT).

3.2 The rationale behind the WPM Policy is clear in that we will accept only those Clients:

- Whose sources of funds can be reasonably established as legitimate; and
- Who do not pose any risk (actual or potential) to WPM's reputation.

3.3 In lieu of our policy, WPM will not tolerate any involvement in illegal activities by its Staff, clients, and/or subsidiaries.

4. POLICY, STATUS, AND SCOPE

4.1 The provisions, procedures, and controls detailed below shall apply to:

- WPM Staff; and
- any WPM client and/or affiliate; and
- any WPM subsidiary company and/or division.

4.2 Breach of the Policy by WPM Staff, clients, affiliates, and/or subsidiary shall constitute a disciplinary offence. As such, WPM reserves the right to take any additional action as it, in its sole discretion, deems fit in securing the diligent and proper implementation and enforcement of this policy.

5. PROCEDURES AND CONTROLS (General)

5.1 This Policy contains certain procedural checks and balances in order to ensure that its vigilant and effective operation are integral components thereof.

5.2 The Procedures & Controls are as follows:

- Identification, Verification, and Know-Your-Customer (KYC) measures;
- Updating of KYC information;
- Automated activity monitoring;
- Reporting of suspicious activities;
- Training and Awareness; and
- Record Keeping.

6. PERIODICAL REVIEW

6.1 Our policies shall be reviewed on regular basis. Any review shall take into account changes provided to WPM related to any and all legislation and guidelines that may affect our operations or our ongoing relationships with our clients.

7. IDENTIFICATION (ID), VERIFICATION (VR) and KNOW-YOUR-CUSTOMER(KYC)

7.1 ID, VR, and KYC together form the first key step in the Procedures and Controls and are to be conducted prior to the granting of any applicant approval for opening a WPM account and/or conducting any business transactions. The carrying out of ID, VR and KYC procedures are vital and necessary for opening an account and commencing any business transactions with WPM. It enables basic background information about the Applicant, their business, source of funds/metals, expected level of activity to be obtained, and outlines the basic elements of our account management guidelines.

7.2 **Where Applicant is a Company seeking to be a WPM client.**
The ID, VR, and KYC process regarding an Applicant Company include but are not limited to the following:

- Corporation or Business Entity name;
- Shareholders;
- Beneficial owners;

- Signatories;
- Country of origin;
- Copy of Government Issued Identification;
- Contact details;
- Previous business activities (type and volumes);
- Anticipated type and volume activities;
- Source of funds;
- Declaration; and/or
- Bank Reference and/or Trade Reference.

7.3 The KYC process must be carried by WPM itself. WPM may seek guidance from domestic and/or international government agencies to carry out the Applicant screening and relative risk assessments.

8. KYC INFORMATION UPDATING

8.1 Reasonable steps must be taken by WPM and the Client to ensure that ID, VR and KYC information is updated regularly and/or when applicable.

9. AUTOMATED ACTIVITY MONITORING

9.1 WPM will monitor the activities of its Clients on regular basis, to ensure that their operations are conducted in accordance with the relevant guidelines related to our common business activities.

10. REPORTING OF SUSPICIOUS ACTIVITIES

10.1 Procedures for AML place a clear obligation on all WPM Management and Staff to report any suspicious activities or information which may point to transactions and instructions being related to illegal activities. Since money laundering and the finance of terrorism methods and guidelines are always evolving, our Compliance Department, along with any relevant guidance from law enforcement and/or other government entities, will inform Staff regarding what are to be considered suspicious activities in both money laundering and financing of terrorism.

10.2 It is the duty of WPM management to report any suspicious activity or information both internally as well as to the appropriate law enforcement or government agency. In doing so, WPM will:

- Provide a reasonable explanation and/or supporting documentation for the suspicion;

 Not be obligated to report the suspicion directly to the Client or Third party; and

 Provide additional information as may be requested by law enforcement or government agency officials.

11. TRAINING AND AWARNESS

11.1 Training shall be carried out on regular basis for all concerned WPM Staff in order to ensure awareness regarding AML and CFT policy, regulations, controls and responsibilities which require their compliance and which form the basis for this Policy.

11.2 All new (or recently hired) WPM Staff will be trained regarding policy, AML, and CFT, as well as proper procedure for reporting suspicious activity and/or transactions. Such introduction may be carried out as part of the normal training procedures.

12. Recordkeeping

12.1 KYC Documentation includes but is not limited to:

 Client documentation and/or correspondence regarding WPM contract;

 Client documentation and/or correspondence regarding WPM account opening;

 Denial of account opening application;

 All documentation related to reporting on suspicious activity concerning a client together with any response/follow up; and/or

 Records of AML/CFT training sessions attended by WPM Staff, their dates, content and attendees.

12.2 Retention Period

All documentation required under this Policy should be retained for a period of at least 2 years from the date of termination of client account.
12.3 Investigation

Where a client is the subject of an investigation of any kind, all documentation relating to the investigation must be retained for such time until the authority conducting the investigation informs WPM.

13. WPM MANAGEMENT and STAFF RESPONSIBILITY

13.1 Scope of Responsibility

In carrying out the proper discharge of their duties under the Policy, both WPM Management and Staff alike will be expected to:

- Assume responsibility for their role with respect to compliance and due diligence issues;
- Ensure their own and their team's awareness of compliance with ID,VR and KYC, record keeping and reporting; and
- Participate in ongoing AML/CFT training as WPM deems necessary from time to time.

Appendix A - Corporate KYC Checklist

The following information/documents may be collected and retained:

A-1 Proof of legal existence of Applicant Company:

□ Trade License (if relevant in country of incorporation);
□ Certificate of Incorporation; and/or
□ Memorandum and Articles of Incorporation.

A-2 Proof of Applicant company's physical address in country of origin and physical address within the United States (when applicable):

□ Original utility bill;
□ Copy of lease/purchase agreement;
□ Original statement from a financial institution; and/or
□ Letter from public authority or external auditor.

A-3 Contact details of Applicant Company:

□ Office telephone number(s);
□ Office fax number(s);
□ Office email address; and/or
□ Website address.

A-4 Proof of Identity of all controlling individuals/shareholders of the Applicant Company

A-5 Contact details of the Company Shareholders:

□ Telephone number(s);
□ Fax number(s); and/or
□ Email address.

A-6 Declaration by authorized signatories of the Applicant Company that the beneficial owners mentioned are the sole beneficial owners of the Applicant Company.

A-7 Identities and addresses of all signatories of Applicant Company.

A-8 Understanding the relationship that exists between the principals of the applicant company and the powers of attorney/third party mandate holders.

A-9 Names and address of all partners in partnerships.

A-10 Details of Applicant Company's line of business including:

□ Main products;
□ Main activities geographical areas; and/or
□ Volume of activities.

A-11 Indication of the anticipated volume and type of activity to be conducted by the Applicant Company.

A-12 Understanding the source of funds originating from the Applicant Company accompanied by Signed Declaration affirming legal source of funds, metals and equity.

A-13 Bank reference whereby Applicant Company has been known to the issuing bank for a reasonable period of time (preferably 1-2 years) or Trade Reference.

If for some reason the information referenced above is not available, WPM reserves the right to conduct a reputational market presence survey approved and signed by the Managing Director.

A-14 External Auditors name and address (if applicable).

Appendix B - Corporate KYC Updating Checklist (For Internal Use)

The following information/documents may be collected and retained as needed:

B-1 Same year proof of physical address of Corporate Client in the form of:

□ Utility bill; and/or

□ Copy of lease/purchase agreement.

B-2 Recent contact details of Corporate Client:

□ Office telephone number(s);

□ Office fax number(s);

□ Office email address; and/or

□ Website address.

B-3 Description of Corporate Client's activities (types and volume) for the last two years.

B-4 External auditors name and address (If Applicable).

Appendix C - Practical Issues Concerning Training and Awareness (Section 12)

C-1 Any training provided must include:

□ An introduction into what is money laundering/financing of terrorism;

□ Developing the ability to recognize suspicious activities or ‘early warning’ signs (particularly regarding commodities trading);

□ The requirements of domestic and international regulatory legislation and their implications; and/or

□ The Policy.

C-2 Training and awareness can be raised through the following tools:

□ Handbooks;

□ Awareness memorandums; and/or

□ Courses (internal and external).

Appendix D - Practical Issues Concerning Record Keeping

D-1 Storage Location

If it is not possible or practicable (for example due to space constraints) to store KYC Documentation on site, then a suitable external location may be utilized.

Suitable external locations may be:

□ A secure area (e.g. warehouse, office) owned and/or operated by WPM; and/or

□ A secure area owned and/or operated by a reputable third party provider.

Regardless as to whether KYC Documentation is stored on or off-site, the documents themselves must be stored in a secure, fireproof location.

D-2 Use of Other Storage Media

As an additional safeguard, the Company may elect to scan images of original documents onto CD-Rom format. CD-Rom's should be stored in a secure environment suitable for the long term storage of electronic/digital media.

D-3 Data Retrieval/Accessibility

The robustness of the security offered by any given storage option should not compromise the efficacy of data retrieval. Storage locations which prevent a reasonably fast retrieval of data should be disregarded in favor of suitable alternatives. The requirement for swift data retrieval is particularly important when dealing with third party conducted investigations where WPM may be requested to source and forward on data within a stipulated time period.

As such, stored KYC Documentation should be indexed by reference to:-

□ Member name;

□ Date stored;

□ Data type (e.g. registration, license, correspondence, report); and/or

□ Details of the individual responsible for filing the KYC documentation in storage.