PRESTIGE PRECIOUS METALS FZCO

ANTI-MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION POLICY (AML/CFT/CPF)

Prepared by :	Compliance Officer		
Approved by:	Managing Director		
Effective Date	12 January 2026		
Version Number	05	**Revision Date**	12 January 2026

PRESTIGE PRECIOUS METALS FZCO P.O.Box 453172 Dubai, UAE

Revision History

Date	Version	Author	Comments (including Review History)
27 July 2023	01	Compliance Officer	Designed to meet the Legal and Regulatory Requirements of United Arab Emirates
15 December 2023	02	Compliance Officer	Amended to meet the UAE regulations and directives on AML/CFT
29 April 2024	03	Compliance Officer	Amended to meet the UAE regulations and directives on AML/CFT
26 June 2025	04	Compliance Officer	Amended to meet the UAE regulations and directives on AML/CFT
12 January 2026	05	Compliance Officer	Amended to include the reform of the UAE 2025 AML/CFT/CPF regulations and directives

AML/CFT/CPF POLICY – SUMMARY

This document summarises the AML/CFT/CPF Policy of Prestige Precious Metals FZCO (Version 05). It does not replace the full Policy: in case of any inconsistency, the full Policy and applicable UAE law prevail.

I. INTRODUCTION AND COMMITMENT

Prestige Precious Metals FZCO (the "Company") is registered with the Dubai Multi Commodities Centre under License No. DMCC-879792 and refines raw gold. As a Dealer in Precious Metals and Stones (DPMS), it is a Designated Non-Financial Business and Profession (DNFBP) under the UAE AML/CFT/CPF framework.

The owner, Senior Management and employees are committed **not** to:

- accept funds or precious metals known or believed to be the proceeds of crime;
- enter into or maintain business with persons or entities known or suspected to be terrorists or criminal organizations, whether or not they are on a sanctions list;
- maintain anonymous or fictitious-name accounts; or
- deal with persons or entities from prohibited jurisdictions or industries.

II. LEGAL AND REGULATORY FRAMEWORK

In 2025 the UAE replaced its previous AML regime (Federal Decree-Law No. 20 of 2018 and Cabinet Decision No. 10 of 2019). The Policy is based on the following instruments:

Instrument	Key relevance for the Company
Federal Decree-Law No. (10) of 2025 (in force 14 October 2025)	Core AML/CFT/CPF law. Makes proliferation financing a distinct offence; brings virtual asset service providers into scope; increases penalties; allows the FIU to suspend suspicious transactions for up to 10 working days and freeze funds for up to 30 days (extendable by the Attorney General); strengthens beneficial ownership rules, including for nominee directors and shareholders.
Cabinet Resolution No. (134) of 2025 (in force 14 December 2025)	Executive regulations setting out the detailed procedural and compliance obligations of DNFBPs, including proliferation financing risk obligations.
Federal Law No. (7) of 2014	Defines terrorism offences and their penalties.
Cabinet Decision No. (74) of 2020	Terrorism lists and implementation of UN Security Council resolutions (Targeted Financial Sanctions).
Cabinet Resolution No. (71) of 2024	Administrative penalties for DNFBPs supervised by the Ministry of Economy and Tourism and the Ministry of Justice.
Cabinet Decisions No. (109) and (132) of 2023	Beneficial owner procedures and penalties for breach of beneficial ownership obligations.

The Company also applies the guidance of the EOCN (TFS and counter-proliferation financing), the MoET AML/CFT Guidelines and Implementation Guides for DNFBPs, the Supplemental Guidance for DPMS (May 2019), MoE Circular No. 08/AML/2021 on DPMS reporting, and the FIU strategic analysis reports.

III. MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

a. Money Laundering

Under Article 2(1) of the Decree-Law, a person commits money laundering if he knows, or there are sufficient indications to believe, that funds are the proceeds of a predicate offence and he intentionally (a) converts or transfers them to conceal their illicit origin, (b) conceals their true nature, source, location, movement or ownership, (c) acquires, possesses or uses them, or (d) helps the offender evade punishment. Laundering typically passes through placement (introducing criminal cash), layering (complex transfers obscuring the audit trail) and integration (re-entry as apparently legitimate wealth).

A predicate offence is any felony or misdemeanour, including terrorist financing, proliferation financing and tax evasion, committed in or outside the UAE where punishable in both countries. All 21 FATF predicate offence categories are criminalised in the UAE.

b. Financing of Terrorism and of Illegal Organizations

Terrorist financing is intentionally providing or collecting funds, by any means including virtual assets, knowing they will be used for terrorism. Unlike money laundering, it follows a linear pattern: funds are raised, stored (including in precious metals), moved and used. Financing of terrorism and of illegal organizations are not subject to any statute of limitations.

c. Proliferation Financing

Proliferation financing is raising, moving or making available funds or other assets for the development or use of weapons of mass destruction and their means of delivery, including dual-use goods. The main risk for the Company is the circumvention of UN Targeted Financial Sanctions through sanctioned jurisdictions, front companies and complex supply chains hiding the true end-user. The Company assesses PF risk alongside ML and TF risk.

IV. UAE NATIONAL RISK ASSESSMENT

The 2024 National Risk Assessment (NRA) rates the overall money laundering threat as medium-high. Fraud and drug trafficking are high threats. The DPMS sector is rated medium-high for money laundering, mainly due to its reliance on cash and data inconsistencies. Residual terrorist financing risk is medium-high, with growing cross-border risks linked to conflict regions. Its findings are built into the Company's own risk assessment.

V. SCOPE, GOVERNANCE AND RESPONSIBILITIES

a. Scope and Disciplinary Consequences

The Policy applies to all employees, officers, affiliates and clients of the Company; any breach leads to disciplinary action.

b. Three Lines of Defence and Compliance Committee

The Company applies a three-lines-of-defence model: Operations (first line), responsible for implementing the AML/CFT/CPF policies and procedures, conducting preliminary customer due diligence, and promptly identifying and reporting suspicious activities or transactions; Compliance (second line), providing oversight, guidance, and support the first line, ensuring that AML/CFT/CPF policies and procedures are effectively implemented and followed; and the Internal/External Auditor (third line) independently tests the controls.

c. Senior Management

Senior Management sets the tone from the top; approves the Policy, governance structure, risk appetite and risk assessment methodology; appoints a qualified Compliance Officer with sufficient authority, independence and resources; allocates adequate human, technological and financial resources; oversees the enterprise-wide risk assessment; attends training; and acts on issues raised by the Compliance Officer and the Auditor.

d. Compliance Officer / Money Laundering Reporting Officer (MLRO)

The Compliance Officer/MLRO must be a member of Senior Management, report directly to it, be independent and free of conflicts of interest, and have sufficient time, systems and staff. Unless otherwise designated, the Company's registered and associated person acts as Compliance Officer. Key responsibilities:

- detect transactions linked to crime; receive and investigate internal suspicious transaction reports and file STRs/SARs with the FIU through goAML;
- act as focal point for the FIU, the Supervisory Authority and other authorities, and respond promptly to their requests;
- monitor the application of the Policy and the risk-based approach, and keep the Policy aligned with new laws, guidance and best practice;
- design, deliver and document the training programme and assess its effectiveness;
- submit semi-annual compliance reports to Senior Management (with a copy to the Supervisory Authority) and brief the Compliance Committee quarterly; and
- ensure that KYC, transaction and STR records are kept for at least five years.

VI RISK-BASED APPROACH AND RISK ASSESSMENT

Precious metals combine high value with easy portability. The Company therefore risk-rates every customer and uses the results to allocate AML/CFT/CPF resources and to set proportionate mitigating measures. Risks are assessed by likelihood and impact, reassessed when the business changes and documented in a risk register. The following factors are considered:

Risk factor	Key considerations
Customer / counterparty	Type of customer; complexity and transparency of ownership; whether regulated; links to PEPs or higher-risk sectors. At enterprise level: target markets, size and growth of the customer base, business model and IT capabilities.
Geographic	Origin of the metal (production or trading hub, adequacy of controls, high-risk or sanctioned country); nationality and residence of the customer; place of transaction and delivery.
Delivery channel	How the customer is introduced and served: walk-in or referral, non-face-to-face, intermediaries, third-party payment processors or VASPs.
Product	Quantity, purity, value, form (raw or processed), portability and anonymity. Mined and artisanal (ASM) gold carry higher risk than fine gold.
Transaction	Size, complexity and payment method (cash, wire, third party); consistency with the customer's profile; unusual urgency, delivery or secrecy requests; stage of the supply chain (extraction, raw trading, refining, wholesale, retail).
NRA and new technologies	NRA findings; risks of new products, practices and technologies (e.g. virtual assets, stablecoins, smart contracts) are assessed before launch and kept under review.

Customer risk	Due diligence level	Approval and file review
Low	Simplified Due Diligence (SDD)	Standard approval; review annually
Medium	Standard Customer Due Diligence (CDD)	Standard approval; review annually
High (or suspicion)	Enhanced Due Diligence (EDD)	Senior Management approval; review every six months

Prohibited relationships: shell companies and shell banks; anonymous or fictitious accounts; persons on the UN Consolidated List or the UAE Local Terrorist List; and prohibited jurisdictions or industries. Where a customer acts as trustee, nominee or agent, the Company verifies the agent and the principal; if the beneficial owner cannot be established satisfactorily, it considers whether to proceed and whether to report.

VII. MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING TYPOLOGIES

Staff must be familiar with at least the following typologies and escalate any matching pattern to the Compliance Officer.

Typology	How it works and what to watch for
MONEY LAUNDERING	
Trade-based laundering	Over- or under-invoicing, fake shipments and fictitious sales contracts used to move illicit or foreign proceeds disguised as precious metals trade. Watch for off-market prices and documents that do not match the goods.
Illicit or conflict gold	Gold from conflict-affected and high-risk areas, unlicensed or artisanal mines is smuggled, given false origin documents, then sold locally or refined and re-exported. Watch for implausible origins, missing export permits and unlicensed suppliers.
Cash placement and structuring	Criminal cash is converted into bullion or used to pay refining fees, often split below AED 55,000 to avoid reporting.
Third parties, nominees and shell companies	Relatives, couriers or professional intermediaries act for others, and shell or front companies with nominee shareholders or directors conceal the beneficial owner.
Layering through corporate flows	Large wires are circulated between related local and foreign entities with no commercial rationale, sometimes with VAT or customs carousel fraud.
Alternative remittance and value storage	Hawala and exchange houses move value outside banks; gold serves as a portable store of value later converted into cash or assets.
TERRORIST FINANCING	
Raise, store, move, use	Funds from donations, charities, crime or business are stored in gold or virtual assets and moved by couriers or informal transfer systems, often in small, frequent amounts. Watch for links to conflict zones or transit countries and activity by persons with no economic profile.
PROLIFERATION FINANCING	
Revenue generation by sanctioned states	Sanctioned states sell natural resources, including gold, through intermediaries to fund weapons programmes. Watch for links to Iran, DPRK or their trading partners.
Front companies and procurement networks	State-linked networks use commercial fronts, overseas agents and trade or diplomatic offices to buy dual-use goods.
Concealing the end-user	Freight forwarders and transshipment hubs are named as consignees to hide the true destination.
Virtual assets	Virtual assets transfer value across borders while avoiding sanctions screening.

VIII KNOW YOUR CUSTOMER AND CUSTOMER DUE DILIGENCE

a. When CDD Applies

CDD is carried out before establishing a business relationship or opening an account; before any transaction with a new customer; for occasional transactions of AED 55,000 or more (single or apparently linked); whenever there is a suspicion of ML/TF/PF; and when there are doubts about previously obtained information. No business is conducted with a customer who fails to provide satisfactory evidence of identity, without prejudice to the obligation to report.

b. Core CDD Measures

- Identify and verify the customer using reliable, independent sources issued by public authorities.
- Identify and verify the ultimate beneficial owner(s) and any person acting on the customer's behalf, including their authority.
- For legal arrangements, identify trustees, settlors, protectors, beneficiaries and any other controlling persons.
- Understand the customer's business, the purpose and intended nature of the relationship and the source of funds.
- Screen the customer, beneficial owners and controllers against sanctions lists and for adverse information.
- Monitor the relationship on an ongoing basis.

c. Documentation

Customer type	Minimum information and documents
Individuals	KYC form; valid Emirates ID (UAE nationals and residents), passport with valid visa (non-residents) or GCC ID; proof of address; full name, date and place of birth, nationality, address and contact details; occupation; expected activity; bank reference; source of funds. Originals are sighted and copies certified "original seen and verified"; each customer receives one unique Customer Registration Number.
Legal persons and arrangements	KYC form; trade license or incorporation documents (attested in the country of Incorporation for non-resident entities); shareholders, beneficial owners, managers and signatories; power of attorney and ID of the authorized signatory; proof of address; last two years' audited financial statements; source of funds; bank reference; company search confirming the entity is not dissolved or struck off.

d. Ultimate Beneficial Owner

The beneficial owner is the natural person holding more than 25% of the shares or voting rights; failing that, the natural person exercising control by other means; and, exceptionally, the senior managing official. If the customer appears to be a nominee or front, the person behind it is fully verified.

e. Non-Face-to-Face Customers and Introductions

Remote onboarding follows the same standards as face-to-face onboarding, supported by independent checks (e.g. verified telephone contact, address confirmation, payment from a UAE-regulated bank). The Company does not rely on third-party information or hearsay: Compliance performs all KYC itself, including for introduced customers.

f. Risk Profiling, Acceptance and Updates

All customers and suppliers are risk-profiled at onboarding and periodically, including screening for PEP status, criminal or terrorist links, sanctions and adverse media. Only Senior Management may accept or continue a high-risk relationship. KYC information is updated at least annually (or bi-annually for high-risk customers) and whenever ownership or other material changes occur. All accepted and rejected customers, with the reasons, are kept in the Client Database.

IX. ENHANCED AND SIMPLIFIED DUE DILIGENCE

a. Enhanced Due Diligence

EDD applies to high-risk customers (e.g. customers based in high-risk jurisdictions, complex or opaque structures, nominee shareholders or directors, high-net-worth customers with unclear source of funds, adverse media), PEPs, high-risk countries, doubts about a risk rating, and red-flag situations. EDD measures include:

- independent verification of identity and ownership, certified documents and additional clarifications;
- detailed enquiry into the purpose of the relationship, the business and the source of funds (with evidence where required);
- Senior Management approval to start or continue the relationship;
- more frequent monitoring and updating, payments only through an account in the customer's name with a regulated institution, and on-site visits where appropriate.

b Politically Exposed Persons (PEPs)

PEPs are persons who hold or held prominent public functions in the UAE or abroad (including senior officials of international organizations), their immediate family members and known close associates. The Compliance Officer establishes and assesses the legitimacy of the PEP's source of funds and obtains Senior Management approval before establishing the relationship, and again when an existing customer becomes a PEP, at each review and upon any unusual material transaction.

c. High-Risk Countries

EDD and any countermeasures required by the National Committee are applied to customers and beneficial owners connected with high-risk countries. Relationships or transactions involving persons from FATF black-

listed jurisdictions must be reported to the FIU and may only be executed three working days after reporting, provided the FIU has not objected.

Simplified Due Diligence (low-risk customers only) allows verification after onboarding, less frequent updates and monitoring, and inferring the purpose of the relationship from its nature.

X. TARGETED FINANCIAL SANCTIONS AND SANCTIONS SCREENING

Targeted Financial Sanctions (Cabinet Decision No. 74 of 2020) require the freezing without delay of funds of persons listed on the UAE Local Terrorist List or the UN Consolidated List, and prohibit making funds or services available to them, directly or indirectly. The Company:

- is registered with the EOCN Notification System to receive listing, de-listing and update alerts;
- screens customers, beneficial owners, controllers, counterparties and suppliers at onboarding, before every transaction, on an ongoing basis and whenever the lists change;
- on a confirmed match, freezes funds without delay and without prior notice, ceases all business and notifies the EOCN within five business days of freezing (Fund Freeze Report in goAML); unresolved potential matches are reported as a Partial Name Match Report and attempted transactions as an STR/SAR;
- notifies the Supervisory Authority of any match (including with former customers), suspected links to listed persons, unresolved false positives and unfrozen funds; and
- implements de-listing and unfreezing decisions without delay.

XI. TRANSACTION AND ONGOING MONITORING

Transactions are monitored to confirm that they are normal for the customer, reasonable and legitimate, using threshold-, transaction-type-, location- and customer-based rules. Unexplained divergence from the expected profile is escalated to the Compliance Officer, who decides whether to reassess the risk or report. Ongoing monitoring confirms consistency with the customer's profile, risk rating and source of funds (and source of wealth for high-risk cases). High-risk customers are subject to enhanced monitoring, including review of supply-chain documentation. Customer files are reviewed every six months for high-risk customers and annually for all others.

XII. RED FLAG INDICATORS

The following non-exhaustive indicators do not by themselves prove ML/TF/PF but require further enquiry or EDD and, where appropriate, escalation to the Compliance Officer:

Category	Examples
Customer behaviour	Reluctance to provide ID, KYC or source of funds; false or misleading information; profile inconsistent with transactions; splitting amounts below reporting thresholds;

Category	Examples
	unusual interest in internal controls or in avoiding reports; sudden increase in bullion deliveries; repeated deliveries by foreign nationals in a short period; transfers among associates without commercial purpose; adverse media.
Company behaviour	Registration in a tax haven while operating elsewhere; frequent name changes; shell structures across jurisdictions; many companies controlled by the same persons or proxies; unclear transport arrangements; large flows unrelated to the business.
Product	Bullion inconsistent with industry standards or declared characteristics; systematic disputes of assay results; unexpected alloys or contaminants; signs of tampering or re-casting.
Payment	Cash payment of refining fees or structured cash deposits; unexplained third-party payers; source of funds cannot be established; funds moved in and out quickly; payments to shell companies; proceeds sent to unknown overseas parties; interest-free loans to foreign parties.
Gold mining	Unlicensed production or trading; gold from areas without mines or licences; unexplained drop in licensed production; equipment inconsistent with an artisanal licence; mining in prohibited areas.
Proliferation financing	Dual-use goods inconsistent with the destination; routing through countries with weak export controls; a freight forwarder as final destination; links to Iranian or DPRK weapons programmes; shipments undervalued compared to shipping costs.

XIII. SUSPICIOUS TRANSACTION REPORTING AND TIPPING-OFF

- Any employee who suspects ML, TF or PF must immediately submit an internal STR to the Compliance Officer.
- The Compliance Officer investigates, documents the findings, informs Senior Management and, where there are reasonable grounds for suspicion, files an STR/SAR with the FIU through goAML without delay, regardless of the amount and without invoking professional or contractual secrecy, and responds to any FIU request for information.
- A decision not to report is documented with its justification. A register of all internal reports (reported or not) is kept, showing the date, the reporting person and the related documents.
- Cash transactions of AED 55,000 or more must be supported by evidence of source of funds (e.g. bank cash withdrawal slip or customs declaration).

Tipping-off is prohibited. No director, officer or employee may disclose to the customer or any third party that a report has been or will be made, or that an investigation is ongoing. Failure to report and tipping-off are criminal offences (see Section XVI).

XIV DEALERS IN PRECIOUS METALS AND STONES REPORT (DPMSR)

Trigger	Requirement
Cash transaction of AED 55,000 or more with resident individuals or non-resident individuals	Collect Emirates ID or passport; file DPMSR in goAML.
Cash transactions with corporate entities amounting to AED 55,000 or more	Collect trade licence and ID of the representative; file DPMSR in goAML.
International wire transfer from or to corporate entities amounting to AED 55,000 or more	Collect trade licence and ID of the representative; file DPMSR in goAML.
Any wire transfer conducted through an exchange house, even if the transaction is within UAE	Collect trade licence and ID of the representative; file DPMSR in goAML.
Transaction between two free trade zone companies settling the payment in USD through international wire transfer	Collect trade licence and ID of the representative; file DPMSR in goAML.
Settlement between a free trade zone company and an onshore company (not part of the same group) in the UAE conducted via international wire transfer	Collect trade licence and ID of the representative; file DPMSR in goAML.

The DPMSR need to be filed on the goAML portal within 2 weeks of the occurrence of a qualified transaction for DPMSR. All related documents are kept for at least five years.

XV TRAINING AND KNOW YOUR EMPLOYEE

All staff, directors and officers receive AML/CFT/CPF training covering legal requirements and job-specific application: new employees within 30 days of joining, and all staff at least annually through refresher training. Each employee signs an acknowledgment of the Policy on joining and annually thereafter.

Before hiring employees, directors, senior management, compliance officers and auditors, the Company checks competence, integrity and conflicts of interest through verification of qualifications and employment history, interviews, a police clearance certificate and a sanctions check.

XVI RECORD KEEPING AND INDEPENDENT AUDIT

The Company keeps for at least five years after the end of the relationship or transaction all CDD and EDD documents, transaction records and correspondence; internal suspicious transaction reports and investigation outcomes (five years from the report); training records; and compliance reports to Senior Management. Records must be complete, retrievable and confidential, and available to the authorities on request.

An independent internal or external auditor, appointed annually as the third line of defence, reviews the AML/CFT/CPF programme, records, internal controls and compliance with the law. Its report sets out deficiencies, a management action plan and an overall opinion, and a written follow-up procedure ensures remediation.

XVII PENALTIES FOR NON-COMPLIANCE

Offence or breach	Penalty
Money laundering (Art. 26-1, 26-2)	Imprisonment of 1 to 10 years and a fine of AED 100,000 to AED 5 million (or the value of the criminal property if greater); if aggravated, AED 1 million to AED 10 million (or twice the value). Attempt is punished as the completed offence.
Terrorist financing / proliferation financing (Art. 26-3, 26-4)	TF: life imprisonment or at least 10 years. PF: temporary imprisonment. Both: fine of AED 1 million to AED 10 million, or twice the value of the criminal property if greater.
Legal persons (Art. 27)	Fine of AED 5 million to AED 100 million, or the value of the criminal property if greater; mandatory dissolution for TF/PF and possible dissolution for ML; personal liability of responsible managers.
Reporting, tipping-off, TFS and BO offences (Art. 28, 29-10, 33, 35-1)	Imprisonment and/or a fine of AED 100,000 to AED 1 million for failure to report an STR; at least AED 50,000 for tipping-off; at least AED 20,000 for breach of TFS instructions or false beneficial ownership information.
Administrative penalties (Art. 17)	Warning; fines of AED 10,000 to AED 5 million per violation; restriction or suspension of managers; suspension of activity; licence revocation.
Cabinet Resolution No. (71) of 2024	Administrative fines per violation, e.g. AED 50,000–200,000 for CDD failures and AED 500,000–1 million for failure to freeze without delay.

XVIII KEY THRESHOLDS AND TIMELINES

Item	Requirement
AED 55,000	CDD on occasional transactions; DPMSR filing for cash (and, for entities, wire) transactions; source-of-funds evidence for cash.
Without delay	STR/SAR to the FIU once suspicion is established; freezing upon a confirmed sanctions match.
3 working days / 5 business days	Waiting period after reporting a transaction with an FATF black-listed jurisdiction (absent FIU objection) / EOCN notification after freezing.
30 days / 6 and 12 months / 5 years	Training of new employees / file review of high-risk and other customers / minimum record retention.