Anti-money laundering (AML), combatting terrorist financing (CTF) Policy

V.1

28/01/2025

APPROVALS AND REVISION HISTORY

The Company has approved this Policies Statements and will periodically review and update, as necessary.

Effective Date	Version	Changes Made	Signatures
28 Jan 2025	1.0	AML-CFT Policy	Laurent Mathiot, CEO Maxime Piccot, Head of Due Diligence

1. INTRODUCTION

1.1 Objectives

Fighting serious abuses of human rights, avoiding contributing to conflict over its supply chain, complying with high standards of anti-money laundering (AML), combatting terrorist financing (CTF), and addressing environmental and sustainability responsibilities are central tenets of the OCIM's operating procedures.

1.2 Scope

This Anti-Money Laundering (AML), Combating Terrorist Financing (CFT) policy is mandatory. It applies to all OCIM operations and activities and defines the rules to be complied with throughout the different steps of the due diligence process.

1.3 Laws and Regulations

OCIM rigorously applies the following regulations designated to prevent money laundering and combat terrorist financing in Switzerland:
- Art. 305 bis and art 305 ter of the Swiss Penal Code;
- Federal Act on Combating Money Laundering and Terrorist Financing (AMLA);
- The Ordinance on combating Money Laundering and Terrorist Financing in banking precious metals trading (OBA-OFDF).

In addition, OCIM complies with the LBMA Responsible Gold & Silver Guidances (LBMA RGG/RSG) and the LPPM Responsible Platinum/Palladium Guidance, to adopt high standards of due diligence in order to combat systematic or widespread abuses of human rights, to avoid contributing to conflict, to address environmental responsibilities and to comply with high standards of anti-money laundering and combating terrorism financing practices.

OCIM also complies with the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas ('OECD Guidance') and with the Swiss Ordinance on Due Diligence and Transparency in relation to Minerals and Metals from Conflict-Affected Areas and Child Labour (DDTrO).

1.4 Regulatory Framework

OCIM is regulated and supervised for Anti-money laundering and combating terrorist financing by the ARIF (Romandy Association of Financial Intermediaries) as a self-regulatory organization (SRO) in Switzerland. The ARIF is recognized by the Swiss Financial Market Supervisory Authority (FINMA).

2. ORGANIZATION AND RESPONSIBILITIES

2.1 Management Oversight

The Chief Executive Officer ("CEO") of OCIM is responsible for the overall ethical culture and behavior of the Company and has ultimate responsibility for the Program. The CEO may delegate the performance of

these responsibilities to the rest of the senior management team. This includes understanding the policies, procedures, controls, and systems in place to effectively manage the Company's compliance risk and to ensure an effective compliance Program is implemented to mitigate those risks.

2.2 Compliance Function

The compliance function is responsible for the day-to-day compliance process and procedures, ensuring processes and procedures are documented and carried out as expected; maintaining all documentation for recordkeeping purposes; and, monitoring completion of initial and ongoing compliance training by all employees.

2.3 Employees

Each employee contributes actively to the fight against money laundering, terrorist financing, contribution to conflict or serious human rights abuse, including child labor, and to address environmental and sustainability responsibilities.

3. RISK-BASED APPROACH

OCIM has a risk-based assessment of its counterparties. Counterparties are categorized into two levels of due diligence: non-high risk or high risk (comprised of high risk and/or PeP). The risk level will determine the level of due diligence and monitoring applied to a customer at on-boarding and on an on going basis. The list of criteria to identify high risk counterparties which require enhanced due diligence is documented in Attachment I.

4. CUSTOMER DUE DILIGENCE

4.1 Identification and verification of the contracting party

Before opening a business relationship which is subject to AML or responsible sourcing, OCIM performs an appropriate customer due diligence. This process comprises the following steps:

- Identification and verification of the contracting party including corporate name, date of incorporation, address.
- Verifies the identity of the contracting party bases on the following documents :

Entities registered in a Business Register	An up-to-date business register's extract delivered by the Business Register or downloaded from the Business Register database or from a reliable private database or from the regulatory body database.
Entities not registered in a Business Register	The articles of association, deed or contract of foundation, an official authorization to exercise the activity, an attestation from the auditors or an equivalent document, or based on an extract from a reliable private database or from the regulatory body database.
Governmental entities	The articles of association or proper decision or on other proper equivalent documents.

When performing the verification of the identity of the contracting party, the business register's extracts or equivalent document should be dated no later than twelve months.

OCIM shall obtain the presentation of the originals or a certified true copy of the documents for the verification of the identity of the contracting party. The certification shall be issued by:

- A public notary or an official authority;
- A Swiss or foreign financial intermediary which is subject to an equivalent AML supervision;
- A lawyer authorized in Switzerland.

OCIM may renounce to the authenticity attestation if other measures are taken to prove the identity and address of the contracting party. Such measures should be properly documented in the due diligence file. If the business register extract is accessible by computer and continuously updated, OCIM may also verify the identity by means of acceding to this official Register, downloading and printing the extract from this Register. In such a case, the documents downloaded shall be dated and countersigned by the employee on the day of their download.

If the identity of a legal entity as contracting party is publicly known, this fact may be documented instead of carrying out the verification of its identity. The identity is deemed to be publicly known specially if the contracting party is a public company or is directly or indirectly associated with a public company.

In the case that OCIM cannot verify the identity based on above listed documents, its identity may exceptionally be verified based on another reliable document. Such derogation must be properly justified in the due diligence file.

4.2 Identification of the ultimate beneficial owner (controlling person) of a legal entity

If the contracting party is a legal entity, OCIM requests a written declaration from the contracting party attesting the individual(s) holding directly or indirectly 10% or more of the contracting partner's shares (capital shares or voting right) and verifies their identity.

If the capital shares or voting rights cannot be determined or in case there are no capital shares or voting rights of 10% or more, OCIM requests a written declaration from the contracting party attesting the person controlling the contracting party in other ways.

In case these persons cannot be determined, or these persons do not exist, OCIM requests a written declaration from the contracting party identifying the managing director(s) of the contracting party. The declaration should provide the following information: Name, first name, address, nationality and date of birth of the identified controlling person(s).

OCIM will not obtain the information on the ultimate beneficial owner (controlling person) when the contracting party is:

- A company listed on a stock exchange or a subsidiary of a company listed on a stock exchange;
- A government entity;
- Swiss banks, portfolio managers, fund management companies, investments funds, securities firms, central counterparties and central securities depositories, insurance and tax exempted pension plans, and payment systems;

- Foreign banks and financial intermediaries subject to an AML-CTF regulatory environment and supervision equivalent to those of the AMLA.

4.3 Know Your Customer ("KYC") information

In addition to the verification of the identity of the contracting party, the identification of the ultimate beneficial owner (controlling person), OCIM collects KYC information based on the risk level of the relationship.

KYC information may include:

- Description of the customer's business activity, including its precious metal sourcing practices, type of precious metal counterparts and main markets;
- Purpose of the relationship;
- Details on the source of funds/wealth;
- Origin of precious metals, including identifying sources of any third-party stock;
- Destination of precious metals;
- Precious metals flow of transactions (including volume, frequency, type and form of precious metals);
- Economic background of the transactions;
- Financial information;
- Standard Settlement Instructions;
- Mining capacity and practices in place;
- KYC information on other key actors of ASM supply chains or supply chain located in conflict or human right abuses high risk areas.

OCIM will as well collect corroborative documentation based on the risk level. Such documentation may include financial statements, AML and supply chain policies, mining license and import/export license.

4.4 Customer Screening

Customer screening of contracting party, its controlling person(s), its beneficial owner(s) and authorized signatory(ies) is mandatory at on-boarding.

Sanctions and PEP identification. Screening might be extended to any other associated parties identified.

4.4 Due Diligence Reviews

Reviews of due diligence information held on counterparties' files are conducted on a periodic basis to ensure that existing customer information remains accurate and up-to-date. Business relationships classified as high risk are reviewed on an annual basis. Business relationships classified as non-high risk are reviewed every 5 years. Due diligence reviews may also be performed when a trigger event occurs during the life cycle of the business relationship.

5. TRANSACTION MONITORING

OCIM monitor continuously the transactions and the account activity for any suspicious or unusual transaction. In particular, the following procedures are applied:

A robust traceability system records supply chain information and documents for each lot. The following specific and relevant transactional information and documents are received and controlled by Operations

for each shipment received, such as type and form of precious metal, shipping documents (airway bills, packing list, pro-forma invoice), export and import form.

Beneficiaries of payments are reviewed by Treasury and Operations before settlement instructions (SSI) are set up in the system to identify any high-risk transactions linked to third party payment.

Each delivery is recorded in a traceability system database recording information and documents linked to the delivery. The Operations Department reviews the shipments received daily and escalates any issue to Executive Management.

The list of criteria defining high risk transaction is documented in Attachment II.

6. REPORTING OF SUSPICIOUS TRANSACTION AND FREEZING OF ASSETS

In the case of a founded suspicion of money laundering after clarifications, the Compliance Department in agreement with a member of the Executive Management Committee submits a report without delay to the Money Laundering Reporting Office. During the analysis done by the Money Laundering Reporting Office, OCIM executes the orders the counterparties only if the transactions are traceable (paper trail).

The assets will be frozen in compliance with art. 10 AMLA. OCIM must not inform the relevant persons or any associated parties that a report has been filed to the Money Laundering Reporting Office.

In addition, OCIM will terminate or suspend its activity with a counterparty if there is a known instance of/founded suspicion of:

- Serious human right abuses;
- Fraudulent misrepresentation of the origin of minerals;
- Direct or indirect support to illegitimate non state armed group;
- ESG catastrophic impact.

7. PROHIBITED ACTIVITIES

In no circumstances will OCIM open an account with a contracting party for which OCIM knows or should know that they finance terrorism, are part of, or support criminal organization.

OCIM will not accept any assets for which OCIM knows or should know come from a crime or a qualified tax offence, even if the crime has been done in a foreign country.

OCIM further prohibits

- Sourcing of precious metal originating from a World Heritage Site;
- Sourcing any material for which OCIM knows or should know that they originate from an illegitimate source;
- Cash settlement of transactions with counterparties.

8. RECORD KEEPING

OCIM retains records of customer due diligence, customer risk level, transactions and clarification obtained for customers or transactions. The documents are retained for 10 years after the termination of the business relationship or after completing the transaction.

9. TRAINING

OCIM is responsible for the training of all employees who have an activity subject to AML. It also establishes the planning and scheduling of the trainings and ensures compliance with the training obligations of OCIM employees.

10. EXTERNAL AUDITS

OCIM is subject each year to external audits in order to verify the compliance with:

- The Swiss AML act.
- The OBA-OFDF.

11. POLICY REVIEW

This Policy shall be reviewed on an annual basis and updated, if necessary, to remain in line with applicable AML, CTF, sanctions laws and regulations and responsible sourcing guidances.

6 mars 2025

Signature

Date

Laurent Mathiot

Maxime Piccot

6 mars 2025

Name (Please print)

ATTACHMENT I : High risk counterparty criteria

List of criteria to identify high risk counterparty :

Location High Risk Criteria	• Precious Metals originate from/has transited via a Conflict Affected and High-Risk Areal. • Precious Metals is claimed to originate from a country through which gold from CAHRAs is known, or reasonably suspected to transit. • Mined Precious Metal is claimed to originate from a country that has limited reserve. • Counterparty or beneficial owner located in a country representing high risk of money laundering and is neither controlled by a listed company on a recognized stock exchange nor by an international group with adequate AML guidelines.
Counterparty High Risk Criteria	• Domiciliary companies not part of a group listed on a recognized stock exchange. • The contracting party, an authorized signatory, the beneficial owner of the assets or the ultimate beneficial owner is a politically exposed person or a close associate/family member of a politically exposed persons. • Involved in high-risk business such as money changer not subject to AML equivalent supervision, arms, gaming, casino industry, antiques and art and sects and their leaders. • Non-LBMA Refinery with high-risk supply chain and with material non-conformance in their OECD guidance equivalent program audit. • Trading entity sourcing Non-LBMA bullion produced by a non LBMA/LPPM, RMI, RJC, CME or LME accredited refineries. • Having significant unexplained geographic routing in their supply chain. • Known to have sourced precious metals from CAHRAs in the last 12 months. • Artisanal Mine. • Mine using mercury

ATTACHMENT II: High risk transaction criteria

List of criteria to identify high risk transaction:

- Third party payment, except if ordered by a financial intermediary subject to an equivalent AML regulatory environment and supervision or with a financial intermediary as final beneficiary;

- Deliveries to a third party, except if ordered by a financial intermediary subject to an equivalent AML regulatory environment and supervision;

- Unusual transaction compared to the expected activity of the business relationship (ex: volume, frequency, type of materials);

- Unusual delivery method of precious metals (use of unusual method of transportation);

- Precious metals come from a conflict affected area.