# ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

Caurum S.r.l. adopts this Policy in compliance with the provisions of Legislative Decree 231/2007 and subsequent amendments, to prevent and combat the use of its economic-financial system for money laundering, the handling of stolen goods, or the financing of international terrorism.
The Company rejects all forms of organized crime and bases its business relationships on the principles of transparency, integrity, and strict adherence to the law. Exposure to AML/CFT (Anti-Money Laundering / Counter-Terrorism Financing) risk poses a direct threat to the Company's stability, financial soundness, and reputation; therefore, compliance with the guidelines set forth herein is mandatory and binding for all employees, members of corporate bodies, and collaborators, as well as—to the extent applicable—business partners and suppliers.

Caurum S.r.l. does not assist, tolerate, facilitate, or participate in any way in transactions that may constitute financial crimes or tax evasion. To this end, the Company formally undertakes to:

- **Strictly refuse** cash payments or commercial transactions whenever there are grounds for suspicion or uncertainty regarding the lawful origin of the funds or assets;
- **Prohibit any conduct** aimed at facilitating the acquisition, substitution, transfer, or control of assets derived from criminal activity;
- **Implement a zero-tolerance policy** regarding any practice of fraud or tax fraud, whether internal or within the supply chain.

To ensure full compliance and manage risk exposure based on a proportionate approach (Risk-Based Approach), Caurum S.r.l. implements the following mandatory operational controls:

## 1. KNOWLEDGE OF THE COUNTERPARTY (KYC)

As previously stated, "Know Your Customer" (KYC) procedures constitute a fundamental aspect of national and European regulations governing financial relationships. Conducting customer due diligence not only serves as an effective tool for combating money laundering and the financing of terrorism but also protects Caurum S.r.l. against commercial and reputational risks, as well as the imposition of administrative, civil, and criminal sanctions.
Caurum S.r.l. carries out customer due diligence and identifies the Ultimate Beneficial Owner by monitoring activity through the analysis of the following parameters:

- Legal nature;

*Reproduction of this document (even in part) is prohibited without the authorization of Caurum Srl*

- Activities performed;
- Conduct at the time of establishing the ongoing relationship or executing the transaction;
- Geographical area of origin;
- Type of transaction or relationship;
- Transaction amount;
- Reasonableness of the transaction and the relationship;
- Reputation in the sector.

As part of its customer due diligence procedures, Caurum S.r.l. conducts a specific check to determine whether the counterparty—or the relevant Ultimate Beneficial Owner—falls into the category of a **Politically Exposed Person (PEP)**. If PEP status is identified, the company is required to apply enhanced due diligence measures, necessitating Senior Management approval to establish or continue the business relationship, as well as continuous and intensified transaction monitoring.

Obtaining this set of customer information—derived from both internal and external data—enables Caurum S.r.l. to determine the money laundering risk profile for each client; this profile is subject to periodic monitoring based on reviews of the established business relationship.

If it is not possible to carry out customer due diligence in compliance with the prescribed standards, Caurum S.r.l. is required to refrain from establishing an ongoing business relationship, executing transactions, or continuing an existing relationship.

## 2. DATA RETENTION

In accordance with Articles 31 and 32 of Legislative Decree 231/2007, Caurum S.r.l. employs record-keeping systems (paper-based and/or electronic) designed to ensure the security, integrity, and confidentiality of data obtained during the customer due diligence process. All identification documents, information regarding the purpose of the relationship, and records of financial transactions will be retained for a mandatory period of **ten years following the termination of the ongoing relationship or the execution of the occasional transaction**, in order to facilitate any subsequent investigations by the UIF or other competent authorities.

*Reproduction of this document (even in part) is prohibited without the authorization of Caurum Srl*

## 3. SIGNALLING OF SUSPICIOUS TRANSACTIONS (SOS)

Caurum S.r.l. employs a structured process for managing reports of potentially illicit transactions. In compliance with applicable regulations, the company formally appoints an **SOS Delegate/AML Officer** (a role held by the Compliance Officer). Employees and suppliers are required to promptly report any anomalies or unusual transactions to the SOS Delegate using internal company channels, including anonymous ones. The SOS Delegate evaluates the anomaly based on the **Anomaly Indicators issued by the UIF (Financial Intelligence Unit)** and, where the necessary conditions are met, proceeds to electronically submit a formal report to the UIF. Caurum S.r.l. does not tolerate retaliation against individuals who speak up about conduct they believe to be unethical, illegal, or inconsistent with company policies—even if the reported issue proves unfounded—provided the report was not made in the knowledge that it was false.

Caurum S.r.l. conducts an internal analysis of detected anomalies. The process entails retaining a record of the evaluation and related documentation, regardless of whether a formal report is submitted to the competent authorities or the anomaly is dismissed as non-suspicious.

## 4. AML GOVERNANCE AND MANAGEMENT OF SUSPICIOUS TRANSACTION (SOS)

Ultimate responsibility for anti-money laundering and due diligence (KYC) policies rests with the Legal Representative of Caurum S.r.l. To ensure maximum operational effectiveness, the Legal Representative formally delegates all decision-making and executive functions to **the Compliance Officer**, who simultaneously assumes the roles of **AML Officer and Suspicious Transaction Report (SOS) Delegate**. This delegation expressly includes the authority to approve the establishment or continuation of business relationships with counterparties classified as high-risk or holding the status of **Politically Exposed Person (PEP)**.

KYC analyses prepared by the internal Compliance Department are submitted to the Compliance Officer/AML Officer, who grants final authorization to proceed with the business and periodically informs the Legal Representative. To ensure compliance with applicable regulations, the Legal Representative guarantees the total independence of the AML Officer, who operates with full autonomy and **sole responsibility** regarding the assessment of anomalies and the potential electronic filing of Suspicious Transaction Reports (STRs) with the Financial Intelligence Unit (UIF), without any obligation to provide prior notification to or obtain authorization from senior management.

*Reproduction of this document (even in part) is prohibited without the authorization of Caurum Srl*

In accordance with Article 39 of Legislative Decree 231/2007, all employees, directors, and collaborators of Caurum S.r.l. are **strictly prohibited** from disclosing to the relevant client or to third parties the fact that a suspicious transaction has been reported, that such a report has been forwarded to the competent authorities, or that an internal investigation is underway. Violation of this prohibition is a criminal offense.

## 5. EMPLOYEE TRAINING AND COMPLIANCE CULTURE

Caurum S.r.l promotes the dissemination of its Anti-Money Laundering (AML) Policy and is committed to raising awareness among all relevant parties regarding compliance with the principles contained therein. External communication is carried out by publishing the AML Policy on the company website, sending it to clients and suppliers alongside due diligence and customer verification questionnaires, and incorporating specific clauses or provisions into agreements with third parties that mandate acceptance of the anti-money laundering principles adopted by the Company.

Regarding internal communication, the AML Policy is distributed—in hard copy and/or electronic format—to every employee, collaborator, and consultant; its principles are further reinforced through periodic communications from the relevant departments concerning the adopted standards of ethics and integrity that must be observed. All employees, consultants, and external collaborators are required to be familiar with and apply AML procedures, properly report suspicious transactions, and participate in mandatory training courses organized annually by the Company.

Caurum S.r.l. recognizes that staff awareness is the primary and most effective safeguard against financial crime. Accordingly, the Company implements a mandatory, continuous, and structured training program for all employees, directors, and collaborators regularly working within corporate functions exposed to AML/CFT risks (including, by way of example: Administration and Finance, Purchasing/Procurement, Sales/Commercial, the Compliance Office, etc.).

Each training session may be delivered externally or internally and conducted online, via e-learning, or in person. The Compliance Officer/AML Officer is responsible for monitoring the plan's implementation and retaining attendance records, course syllabi, and certificates of

*Reproduction of this document (even in part) is prohibited without the authorization of Caurum Srl*

completion **for 10 years, to demonstrate compliance with training** obligations to supervisory authorities.

## 6. DUE DILIGENCE INTEGRATION – RAW MATERIAL SUPPLY CHAIN (CONFLICT MINERALS)

Given Caurum S.r.l.'s field of operation and for the purposes of managing the risk of corruption, fraud, and money laundering, the Company aligns its procurement procedures with the standards of EU Regulation 2017/821 and OECD guidelines.

Depending on its position in the supply chain, the company commits to monitoring upstream suppliers to prevent the introduction into the market of raw materials linked to conflict or human rights violations, reserving the right to immediately suspend or terminate relationships should risk mitigation efforts fail.

Any report of a violation of this Policy may be submitted via the company's web platform https://www.caurum.com/whistleblowing/, compliant with the confidentiality requirements of the **D. Lgs. 24/2023 (Whistleblowing)**, or by writing to the dedicated email address: odv231@caurum.it.

This policy is reviewed annually

San Zeno, 15/09/2026

The Chief Executive Officer

*Reproduction of this document (even in part) is prohibited without the authorization of Caurum Srl*