ANTI-MONEY LAUNDERING POLICY

APPROVED BY PYSMIAN S.p.A BOARD OF DIRECTORS ON February 10th, 2026

prysmian

The planet's pathways

TABLE OF CONTENTS

LEADERSHIP MESSAGE 2

1. Purpose & Objective 3
2. Policy Owner 3
3. Applicability 3
4. Your Responsibility 4
5. AML Laws and Regulations 4
6. Policy Requirements – Rules of conduct 5

6.1 Use of bank accounts 5

6.2 Checks on Business Partners 6

6.2.1. Customer and Sales Agent Verification 6

6.2.2. Vendor verification 7

6.2.3. Third-Party Payers 7

6.3. Manual Payments 8

7. Consequences of Policy Violation 8
8. Reporting a Policy Violation 8
9. Audit, Monitoring and continuous improvement 9
10. Related Documents 9

LEADERSHIP MESSAGE

As a global manufacturing leader, Prysmian is committed to conducting business with the highest ethical standards and in full compliance with international laws and regulations. Our Anti-Money Laundering (AML) Policy reflects this commitment and reinforces our zero-tolerance approach to financial crime.

Money laundering poses a serious threat not only to the global financial system but also to the trust our customers, partners, and communities place in us. That is why we have implemented controls to detect, prevent, and report any suspicious activity across all our operations worldwide.

Relevant Parties play a vital part in upholding our AML standards. Through a shared sense of responsibility, we can protect our company and contribute to a safer, more transparent global economy.

We count on your dedication and integrity to ensure that Prysmian remains a trusted and compliant partner in every market we serve. Together, we can make a meaningful difference.

Thank you for your commitment to integrity and safeguarding our reputation.

Massimo Battaini
Prysmian CEO

1. PURPOSE & OBJECTIVE

Money laundering is the process of concealing the true ownership and origin of financial assets, making illicit funds appear to have come from legitimate and legal sources. The methods and channels used to launder money are varied and complex. While most illegal proceeds are funneled through financial institutions, criminals may also engage in *trade-based money laundering (TBML)* – a technique that achieves similar outcomes by exploiting non-financial business transactions.

Prysmian is committed to complying with all applicable laws and regulations in every country where it operates or has business relationships. In this regard, all Prysmian employees must follow the Anti-Money Laundering ("AML") Policy and all applicable AML laws in the countries in which they are employed or active, whichever is more restrictive.

The risk of being involved in money laundering should not be overlooked or underestimated. A lack of effective control systems to detect such activities can expose Prysmian companies to the risk of committing money laundering crimes or to the risk of being involved in a money laundering process, even without any active participation in the unlawful conduct.

This Policy outlines the minimum general standards of internal AML controls that Prysmian companies must follow to mitigate any legal, regulatory, reputational, and potential financial risk.

2. POLICY OWNER

Group Compliance owns this Policy and is responsible for periodically reviewing and updating it to ensure it accurately reflects organizational updates or legal and regulatory changes.

3. APPLICABILITY

This Policy applies to all employees, interns, officers, directors and administrators of all legal entities of Prysmian, hereinafter referred to as "Relevant Party".

4. YOUR RESPONSIBILITY

This Policy requires you to:

1) Read, understand, and comply with the requirements included in this Policy;
2) Report immediately to the appropriate channels outlined in Section 6 of the **Helpline Policy** any alleged violation of this Policy, both if committed by a Prysmian employee or an external stakeholder;
3) Ask questions or report any concerns related to this Policy to the Helpline Channel;
4) Complete assigned training related or connected to this Policy when required.

5. AML LAWS AND REGULATIONS

All employees, interns, officers, directors, and administrators of all legal entities of Prysmian must adhere to all applicable AML and Counter-Terrorism Financing ("CTF") regulations in the countries where the Group operates.

As an Italian-headquartered company, the Group aligns its practices with the Italian national AML framework, primarily governed by Legislative Decree No. 231/2007, and with the evolving European Union AML regulations.

Given its global footprint, the Group also ensures that its subsidiaries comply with relevant local laws, drawing on international standards such as those promoted by the Financial Action Task Force ("FATF"). This includes, for example, regulatory frameworks in jurisdictions like the United States (including the *Bank Secrecy Act* and the *USA PATRIOT Act*) and the United Kingdom (including the *Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017*, as amended).

The Group adopts a risk-based approach to AML compliance, ensuring that internal procedures are consistently applied while remaining adaptable to local legal requirements.

6. POLICY REQUIREMENTS – RULES OF CONDUCT

Prysmian Companies must make every effort to ensure that no business relationship poses the risk of being part of criminal activities. Prysmian relevant parties are required to take all necessary actions to minimize the risk of participating in money laundering or terrorism financing schemes. This includes conducting an appropriate level of evaluation before entering into any business relationship.

The following sections outline the key AML risk areas pursuant to this Policy.

Where significant AML risks are detected, the relevant Function must escalate the matter to Group Compliance, Group Finance and/or Group Administration for appropriate analysis and further action.

6.1. USE OF BANK ACCOUNTS

A significant portion of global money laundering activities are carried out through the financial system. In many cases, trade-based money laundering techniques exploit the financial system by using various money transmission instruments, such as wire transfers.

In order to reduce the risk of being involved in a criminal scheme:

1) All Prysmian Companies must use bank accounts only with reputable, international financial institutions and the opening and use of such accounts must always be authorized by the Group Finance Department;
2) Any of the following discrepancies identified in the bank accounts used for receiving or making payments must be flagged as potential red flags and addressed accordingly:
    a. The owner of the bank account differs from the name of the business partner;
    b. The bank account is in a different country than the business partner;
    c. The business partner is located in a Red Flag country, as defined by the Group Export Control Procedure.

6.2 CHECKS ON BUSINESS PARTNERS

In accordance with the Third-Party Procedure and the Export Control Procedure, background checks and general due diligence must be conducted for the following categories of third-parties:

1) Customers;
2) Vendors;
3) Distributors;
4) Sales Agents

Before establishing any business relationship, the relevant Functions must:

1) Identify and document the true identity of the potential business partner (e.g. through the company registrations) and ensure that up-to-date information is maintained;
2) Assess whether the size and structure of the counterparty is appropriate and proportionate to the intended business relationship;
3) Evaluate potential risks, such as the engagement in activities that may be considered fraudulent.

6.2.1 Distributor, Customer and Sales Agent Verification

Sales departments across all Prysmian entities are expected to make every effort, prior to establishing any business relationship, to verify customers by requesting the following minimum set of information:

1) its ultimate beneficial owner;
2) any third party involved in the transactions (e.g. a third payer);
3) the end user, if different from the customer.

In addition to the above, customers such as distributors, resellers and wholesalers must undergo the screening process outlined in the Third Party Procedure. This process must also be applied to Sales Agents.

6.2.2. Vendor Verification

The Procurement Function must perform screening activities whenever engaging with specific categories of vendors – such as scrap dealers, freight forwarders, logistics service providers, consultants, and others – in line with the Third Party Procedure. These screenings must be performed using the dedicated platform adopted across the Group, and, where applicable, supplemented by other specialized software or databases available to local subsidiaries.

A key component of this process is the completion of the questionnaire in which the vendor must provide accurate information regarding the identification of its Ultimate Beneficial Owner ("**UBO**"). This step is essential to ensure compliance with AML requirements and to mitigate both reputational and regulatory risks.

6.2.3. Third-Party Payers

If Credit Management, Finance or any other relevant Function, based on the local organizational structure, receives a proposal to involve a third-party payer who is not related to the customer, it must take all reasonable steps to verify the third party before approving the transactions, in accordance with applicable AML principles. This verification may include collecting company information, corporate registry documents, and other reliable sources to confirm the payer's identity and legitimacy.

If the request to involve a third-party payer is addressed to a different Function, that Function must promptly notify Credit Management and/or Finance.

6.3. MANUAL PAYMENTS

Manual payments – such as those for taxes, fines, insurance, membership fees (no invoice is issued), customs charges, advance payments on orders, and donations – are considered exceptions to the standard procedure and must only be used under specific, well-justified circumstances.

Prysmian entities must ensure a minimum level of control over manual payments. Local Finance and/or Administration functions, depending on the organizational structure and roles involved in the payment process, are responsible for implementing appropriate checks and validations to mitigate financial crime risks and ensure compliance with applicable AML regulations.

7. CONSEQUENCES OF POLICY VIOLATION

As a Prysmian Relevant Party, you are agreeing to uphold our commitment to ethical conduct and integrity and to abide by our Code of Ethics. Prysmian employees who violate this commitment or do not comply with this Policy shall be subject to disciplinary procedures, including possible dismissal, and any other legal action required to protect the interest and reputation of Prysmian, in line with the applicable legislation.

8. REPORTING A POLICY VIOLATION

As a Prysmian Relevant Party, you are required to report any Policy violation to:

1) The **Integrity First Helpline**; or
2) Your Regional Compliance Team or the other designated subjects mentioned in Section 6.1 of the Prysmian **Helpline Policy**.

Any form of retaliation, including threats and attempts of retaliation, is strictly prohibited. Prysmian is committed to ensuring that all Relevant Parties are free to disclose any violation, either real or suspected, of the Prysmian's Code of Ethics or any other Company policy or procedure, to the extent they have reasonable grounds to believe that the matters reported

are true. You will not be adversely impacted or retaliated upon in the workplace, either personally or professionally, for raising a valid and legitimate concern.

9. AUDIT, MONITORING AND CONTINUOUS IMPROVEMENT

The Owner of this Policy is responsible to perform periodic reviews and updates of this document, examining, in particular, revisions to be made based on internal organizational updates, changes to external legislation and best practices.

Using a risk-based approach, on a periodical basis the Group Compliance Function and the Internal Audit Department may perform, respectively, monitoring or audit activities aimed at verifying the correct enforcement of this Policy within the organization.

10. RELATED DOCUMENTS

The following Documents are related to this Policy and must be consulted by all Prysmian employees for further guidance. Part of such documents are available in the Ethics & Integrity Section of the **Prysmian Intranet** and are also publicly available within the correspondent Section of the **Prysmian website.**

1) **Code of Ethics;**
2) **Third Party Procedure;**
3) **Export Control Policy;**
4) **Helpline Policy.**