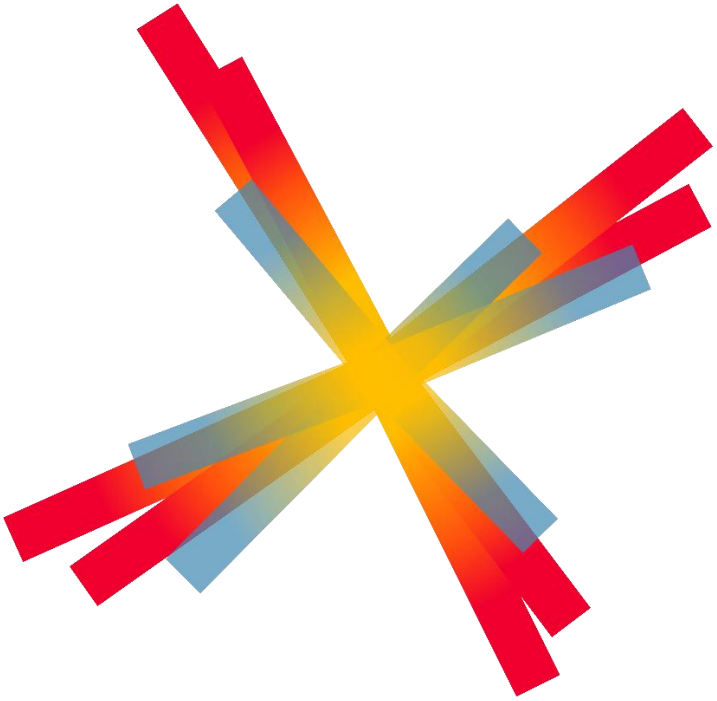
PUBLIC



Anti-Money Laundering Policy

PCO.01.09

2025

sdworx

1. Introduction

1.1 Purpose

SD Worx is committed to high standards of Anti-Money Laundering ("AML") and Combating the Finance of Terrorism ("CFT") compliance, as well as preventing Proliferation Financing. The purpose of this policy is to outline the AML/CFT framework throughout the SD Worx group in accordance with applicable laws, directives and regulations. SD Worx requires management and employees to adhere to this framework to prevent money laundering or terrorism financing using its products and services.

1.2 Scope

The Anti-Money Laundering policy established the standards SD Worx will apply in its obliged entities to prevent and detect money laundering and terrorist financing.

1.3 Policy applicability:

This Policy applies to all workers of the SD Worx' group entities (such term must be construed to include those bound to SD Worx by an employment contract but also other assimilated persons acting on SD Worx' behalf, including without limitation temporary workers and members of the board of directors).

2. General information

2.1 Legal framework

The legal framework for the prevention of money laundering and terrorist financing should be considered at two levels – global and domestic. In the creation of its Anti-Money Laundering policy, SD Worx based itself on the applicable laws, directives and regulations from both levels.

3. Governance

The Anti-Money Laundering Office (AMLO) within Group Internal Control & Compliance falls under the supervision of the Head of Internal Control & Compliance, who reports directly to the Chief Legal & Compliance Officer and provides activity reports to the Audit & Risk Committee on a quarterly basis. When required, AMLO is authorised to contact the Audit & Risk Committee directly.
The AMLO is responsible to:

- monitor which SD Worx group entities are Obliged entities (in collaboration with Regulatory Compliance Team);
- maintain for the SD Worx AML/CFT framework; and

- implement of the AML/CFT framework in Obliged entities.

4. Minimum AML standards

Following standards are the minimum standards that all obliged entities need to implement and will be complemented with more elaborate local process descriptions.

4.1 Business-Wide Risk Assessment

As part of its risk-based approach, SD Worx will conduct a Business-Wide Risk Assessment (BWRA) to identify and assess the Money Laundering and Terrorist Financing (ML/TF) risks related to its products and services, considering:

- the customer receiving the services,
- the duration, type of and delivery channel of services provided,
- the jurisdictions SD Worx operates in.

The Business-Wide Risk Assessment is documented and kept up-to-date.

4.2 Know Your Customer (KYC)

4.2.1 Establishing and verifying the identity

Before entering a business relationship with a prospective customer, the identity of each customer as well as the identity of customer's legal representatives and ultimate beneficial owners must be established with a high degree of certainty through:

- the collection of relevant information to be able to establish the identity of customers as well as the identity of customers' legal representatives and ultimate beneficial owners with reasonable certainty (*identification*)
- the verification of all or part of the identification data against one or more supporting documents or reliable and independent sources of information which enable the data to be confirmed to have a sufficient degree of certainty as to the identity of the persons involved (*identity verification*).

More detailed information regarding the Customer identification and identity verification can be found in the Customer Due Diligence Guidance.

4.2.2 Individual risk assessment

Before entering a business relationship with a customer, key characteristics of the customer and of the business relationship must be identified to categorize the customer in the relevant risk category and determine the appropriate degree of intensity of due diligence measures (at onboarding and in the context of the ongoing vigilance requirements).
The caracteristics include:

- size and complexity of the customer,
- the identity of the customer or of its representatives or beneficial owners,
- the customer's structure,
- any other information collected as part of the due diligence applied to the customer and the business relationship, including the monitoring of transactions.

The individual risk assessment shall be documented.

4.3 Ongoing vigilance requirements

Business relationships can change and therefore need to be continuously monitored.

4.3.1 KYC review

Periodic and risk-based reviews shall be carried out to ensure that the relevant customer documents, data and information are kept up to date.

4.3.2 Transaction monitoring

An adequate and risk-proportionate examination must be conducted of the transactions carried out over the course of the business relationship and the facts surrounding the business relationship or transaction to identify suspicious activity that deviate from the expected behaviour.
SD Worx has established clear internal guidelines detailing on suspicious activity reporting (SAR).

4.3.3 Sanctions

The SD Worx Sanctions policy (PCO.01.07) defines the standards and control mecanisms to manage exposure to sanction risk.

4.4 Investigation and reporting requirements

Where due diligence or ongoing vigilance applied to the customer and their transactions reveal facts or transactions that are atypical in the light of the characteristics of the customer or the nature and purpose of the business relationship, those facts or transactions must be investigated internally by the MLRO and, if the suspicion remains, reported to the relevant authorities. Under no circumstances shall the customer, their representatives, their beneficial owners or any third party be informed that:

- an internal ML/TF analysis is being or may be carried out with respect to the customer or any of its transactions,
- a report is being, will be or has been submitted to MLRO,
- external analyses are being, have been, or may be performed by the MLRO or by the judicial authorities.

5. Organisational measures

5.1 Processes and procedures

As a complement to this policy, SD Worx has established the required processes and procedures, detailing the operational steps to be taken as part of the AML framework. They are distributed to all relevant stakeholders.

5.2 Training and awareness

The AMLO draws up and implements an annual programme for the training and awareness raising of the staff. That programme divides the staff members into different categories (e.g. sales, customer support) and it is tailored to the training needs of those categories of staff (e.g. high-level identification and determination of acceptable residual risks vs. day-to-day implementation of due diligence measures).
The programme is approved by senior AML-management. The AMLO reports on the implementation of the programme as part of its annual activity report.
As part of the training programme, the AMLO ensures that all the employees are made aware of the existence of an internal whistleblowing system.

5.3 Whistleblowing

The SD Worx Whistleblowing policy (PCO.03.02) outlines its secure whistleblowing system to enable our staff to report breaches of the AML/CFT Law on an anonymous basis. More information about the process and a safe reporting channel can be found here.

5.4 Following legal changes

In collaboration with Regulatory Compliance, and as part of its continuous training, the AML Office will monitor applicable AML/CFT laws, regulations and best practices. Where needed, the AML office will update its AML framework to reflect this change.

5.5 Outsourcing of the due diligence

The obligation to perform the due diligence may be outsourced to a third party. This does not impact the fact, that the ultimate responsibility for the fulfilment of this duty remains with the SD Worx obliged entity, who must ensure that at a minimum, all relevant SD Worx policies, processed and procedures are adhered to.

5.6 Data and document retention

All information and documents collected or drawn up for the purpose of implementing the customer due diligence and ongoing vigilance measures is retained in line with applicable laws.

Definitions

Term	*Definition*
AMLO	Person appointed as anti-money laundering compliance officer
Money Laundering Reporting Office ("**MLRO**")	The reporting office for the submission of a suspicious money laundering report
Obliged entity	An entity subject to AML/CFT obligations under applicable national legislation
Senior AML Management	A collegial body consisting of Chief Legal & Compliance Officer and Head of Internal Control & Compliance.

Document control and revision history

Document Title	Anti-Money Laundering Policy
Document Number	PCO.01.09
Policy Effective Date	1/10/2025
Information Classification	Internal
Information Owner	Group Internal Control & Compliance
Document Approver	Risk, Security & Compliance Board
Applicability	SD Worx group
Last review	30/09/2025
Next review date	30/09/2026
Version	1.0

Revision History

Date	*Author*	*Version*	*Changes*
26/09/2025	GICC	1.0	Initial version

Document References

Nr	*Document title*	*Document number*
1	SD Worx Sanctions policy	PCO.03.07
2	SD Worx Whistleblowing policy	PCO.03.02