

Westward Way Tech N.V.



AML & KYC Policies

2025

Content

1. **Introduction & Purpose**
 - Objectives and regulatory alignment
2. **Scope & Applicability**
 - Covered entities, staff, and partners
3. **Governance & Responsibilities**
 - Board, Compliance Officer, Employees
4. **Customer Due Diligence (CDD) & Enhanced Due Diligence (EDD)**
 - Identity verification
 - High-risk customers (PEPs, high-risk jurisdictions)
5. **KYC Procedures**
 - Onboarding and verification methods
 - Ongoing reviews
6. **Transaction Monitoring & Thresholds**
 - Red flags and monitoring
 - Thresholds (e.g., **ANG 4,000**)
7. **Suspicious Transaction Reporting (STR)**
 - Reporting process and no “tipping off”
8. **Record Keeping & Data Protection**
 - Retention periods and privacy compliance
9. **Employee Training**
 - Initial and ongoing training requirements

1. Introduction & Purpose

This policy demonstrates the company's commitment to preventing and detecting money laundering (ML) and terrorist financing (TF). It ensures compliance with international standards and local regulations, while protecting the company, its customers, and the wider financial system.

2. Scope & Applicability

The policy applies to:

- All employees, contractors, and relevant business partners.
- All products, services, and jurisdictions where the company operates.
- Third parties engaged for KYC/AML functions, such as verification service providers.

3. Governance & Responsibilities

- **Board of Directors:** Provides oversight and approves AML/KYC strategy.
- **Compliance Officer (MLRO):** Implements and monitors the program, reports suspicious activities, and communicates with regulators.
- **Employees:** Must comply with procedures, complete training, and escalate red flags.
- **Internal Audit:** Reviews the effectiveness of the program on a regular basis.

4. Customer Due Diligence (CDD) & Enhanced Due Diligence (EDD)

- **CDD:**
 - Verify customer identity using reliable documents (passport, ID card, proof of address).
 - Confirm age and eligibility before granting full access.
- **EDD:**
 - Required for high-risk customers, such as politically exposed persons (PEPs) or customers from high-risk jurisdictions.
 - Additional checks may include source of funds and source of wealth.
- **Ongoing Due Diligence:** Continuous monitoring and periodic refresh of customer information

5. KYC Procedures

- **Onboarding:** Identity verification must be completed before large transactions or withdrawals.
- **Thresholds:** Any single or cumulative transaction exceeding **ANG 4,000** requires verified identity.
- **Verification Methods:** Accepted documents include government-issued IDs and recent utility or bank statements; digital verification may be used.
- **Periodic Reviews:** Customer records must be updated at defined intervals based on risk profile.

6. Transaction Monitoring & Thresholds

- **Monitoring:** All transactions are continuously monitored to detect unusual activity, including patterns that may indicate structuring or attempts to avoid detection.
- **Indicators:** Red flags include repeated small deposits, rapid movement of funds, inconsistent behavior compared to a customer's profile, or use of multiple accounts.
- **Thresholds:**
 - When customer activity **reaches or exceeds defined reporting levels** (e.g., equivalent to a few thousand guilders or local regulatory thresholds), enhanced verification and review are required.
 - Both **single large transactions** and **multiple smaller transactions with a combined effect** are subject to monitoring.
- **Escalation:** Any transaction that cannot be reasonably explained by the customer's profile must be escalated to the Compliance Officer for further assessment.

7. Suspicious Transaction Reporting (STR)

- **Internal Reporting:** Employees must promptly escalate suspicious activity to the Compliance Officer.
- **External Reporting:** The Compliance Officer is responsible for filing Suspicious Transaction Reports (STRs) with the relevant authority.
- **Confidentiality:** Customers must not be informed ("no tipping off") when a report is filed.
- **Timeliness:** Reports must be submitted without undue delay once suspicion is confirmed.

8. Record Keeping & Data Protection

- **Retention:** All customer identification records, transaction data, and compliance reports must be kept for at least **5–7 years**, in line with legal requirements.
- **Security:** Records must be stored securely to prevent unauthorized access or misuse.
- **Data Privacy:** Handling of customer data must comply with applicable data protection laws (e.g., GDPR).

9. Employee Training

- **Initial Training:** All new employees must receive AML/KYC training before handling customer transactions.
- **Ongoing Training:** Regular refresher sessions ensure staff remain aware of risks, regulations, and reporting procedures.
- **Content:** Training includes identification of red flags, reporting obligations, and role-specific responsibilities.
- **Testing:** Employees may be assessed to ensure comprehension and compliance.