Anti-Money Laundering (AML) Policy Template

WWW.HPTGROUP.COM
12 RUE LE CORBUSIER, 1208 GENEVA, SWITZERLAND

1. Policy Statement

This Anti-Money Laundering (AML) Policy outlines the framework, responsibilities, and procedures implemented to detect, prevent, and report money laundering and terrorist financing, in line with:

- Financial Action Task Force (FATF) Recommendations
- EU Anti-Money Laundering Directives (AMLD)
- Relevant national legislation and regulatory obligations

The institution applies a zero-tolerance approach to financial crime and the misuse of its services for illicit purposes.

2. Objectives

- Prevent the misuse of services for money laundering or terrorist financing
- Comply with all applicable AML/CTF obligations
- Define staff responsibilities and internal AML controls
- Detect and report suspicious activities
- Maintain accurate AML records and ensure ongoing training

3. Scope

This policy applies to:

- All employees, officers, and agents
- All operational units, branches, and affiliates
- All clients, intermediaries, and counterparties

4. Risk-Based Approach (RBA)

A Risk-Based Approach is adopted to ensure appropriate controls are applied proportionally to risk exposure. This includes:

- Risk assessments for clients, jurisdictions, and services
- Customer Due Diligence (CDD) adapted to risk levels
- Enhanced Due Diligence (EDD) where high risk is identified
- Ongoing monitoring based on transactional behavior and profile

5. Customer Due Diligence (CDD)

CDD must be conducted at onboarding and updated periodically. Key components:

- Identification and verification of individuals and entities
- Establishment of beneficial ownership (25%+ or control-based)
- Understanding of business purpose and relationship context
- Screening against sanctions, PEP, and adverse media

CDD Triggers include:

- Account opening
- Suspicion of criminal activity
- Material change in client structure
- Regulatory or internal audit requirements

6. Enhanced Due Diligence (EDD)

EDD applies to high-risk clients or relationships, including:

- Politically Exposed Persons (PEPs)
- Clients from FATF-listed jurisdictions
- Trusts, shell companies, bearer share structures
- Large or complex transactions
- Non-face-to-face onboarding

EDD measures include:

- Source of funds and source of wealth verification
- Senior management approval
- Additional documentation and monitoring

7. Ongoing Monitoring

- All relationships are subject to risk-based transaction monitoring
- Patterns inconsistent with expected behavior are flagged
- Alerts are reviewed and escalated to the MLRO (Money Laundering Reporting Officer)
- Periodic risk reassessment is mandatory

8. Record Keeping

Records are retained for at least five years following the end of the relationship or transaction. This includes:

- Identification and verification documents
- CDD/EDD documentation
- Transaction logs and correspondence
- Suspicious Activity Reports (SARs) and internal memos

9. Reporting Obligations

Internal Reporting:
All staff are obligated to report suspicious activity to the MLRO using the internal SAR form.

External Reporting:
The MLRO assesses reports and, if appropriate, submits them to the relevant Financial Intelligence Unit (FIU) or supervisory authority.

10. Training and Awareness

- AML training is mandatory upon onboarding and annually thereafter
- High-risk departments receive enhanced training
- Training covers typologies, red flags, escalation, and responsibilities
- Records of training attendance are maintained

11. Sanctions Compliance

All clients, transactions, and beneficial owners are screened against major international sanctions lists:

- UN Security Council
- U.S. OFAC
- EU Sanctions List
- UK OFSI

Engagement with sanctioned individuals or entities is strictly prohibited.

12. Responsibilities

Role	Responsibility
Board of Directors	Approve and oversee AML framework
MLRO	Implement AML program, assess reports, file SARs
Compliance Department	Conduct CDD, monitoring, training, and internal assessments
All Staff	Adhere to policy, report suspicious activity, attend training

13. Policy Review

This policy is reviewed annually, or earlier if:

- Legal or regulatory updates occur
- Internal audit findings require amendment
- New typologies or risks are identified

14. Disciplinary Measures

Failure to comply with this policy may result in:

- Termination of employment or contract
- Regulatory notification
- Civil or criminal liability under applicable law

15. Declaration

All clients, partners, and staff must provide full cooperation with AML procedures. Refusal to comply with verification or reporting requirements may result in termination of services.
Policy Owner: Compliance Department
Approved By: Board of Directors
Review Date: [Insert Date]
Version: [Insert Version No.]

Role	Responsibility
Board of Directors	Approve and oversee AML framework
MLRO	Implement AML program, assess reports, file SARs
Compliance Department	Conduct CDD, monitoring, training, and internal assessments
All Staff	Adhere to policy, report suspicious activity, attend training