AML and Fraud Management Procedures

VoltEnt

DOCUMENT CREATION	
Version	1.1
Date Created	01 December 2024
Author(s) of Document	Michał Imiołek
Purpose of Document	This Policy sets out the framework for VoltEnt B.V. ("the Company") to prevent the use of its services for money laundering (ML), terrorist financing (TF), and proliferation financing (PF). It reflects the Company's commitment to comply with, and the means by which all transactions are monitored to avoid fraudulent activities.
Authorised By	eMoore N.V, Managing Director and company Compliance Department

CHANGE CONTROL				
Version	**Date of Issue**	**Author(s)**	**Brief Description of Changes**	**Approved By**
1.0	01 December 2024	Michał Ziobro	Initial Release	Maria Bon
1.1	01 May 2025	Michał Ziobro	Updated document as per procedures changes	Maria Bon

1. Purpose and Legal Basis

This Policy sets out the framework for VoltEnt B.V. ("the Company") to prevent the use of its services for money laundering (ML), terrorist financing (TF), and proliferation financing (PF). It reflects the Company's commitment to comply with - Reference to Applicable Laws and Regulations:

- The National Ordinance on the Reporting of Unusual Transactions (NORUT)
- The National Ordinance on Identification when Rendering Services (NOIS)
- Relevant provisions from the Curaçao Gaming Authority (CGA)
- Guidance provided by the Financial Intelligence Unit (FIU) Curaçao

This Policy also integrates standards and obligations under:

- Financial Action Task Force (FATF) Recommendations
- EU 5th and 6th AML Directives (insofar as they inform best practices)
- Wolfsberg Group Principles
- Basel AML Index benchmarks

This Policy also governs the implementation of the Internal Instruction on AML/CFT Procedures, which forms **Annex 1** of this document.

2. Relevance of Detection and Deterrence of Money Laundering and Terrorist Financing

The Company acknowledges its critical role in detecting and deterring money laundering, terrorist financing, and other forms of financial crime. The objective is to prevent the use of our assets for illicit purposes, safeguard the integrity of the financial system, and comply with national and international legal frameworks. These obligations are essential to protecting both the Company and the broader public from criminal exploitation.

3. Appointment of Compliance Officer and Responsibilities

The Company has appointed a Compliance Officer (CO), who is responsible for:

- Overseeing AML/CFT compliance
- Conducting ongoing monitoring and reporting of suspicious transactions
- Liaising with FIU Curaçao and regulatory bodies
- Ensuring timely updates of internal policies and staff training
- Reviewing the BRA at least annually or upon material changes

4. Scope and Objectives

This Policy applies to all employees, departments, and systems of VoltEnt B.V. and governs relationships with all clients and third parties. The main objectives are:

- To prevent VoltEnt from being used for ML, TF or PF.
- To comply with Curaçao AML/CFT/CFP laws and Central Bank guidelines.
- To define the structure of internal AML/CFT governance and monitoring.
- To establish the roles and responsibilities of the Compliance Officer and senior management.
- To outline risk-based measures for due diligence, record keeping, and training.

3. Governance and Responsibilities

Board of Directors and Senior Management: Responsible for approving and overseeing AML/CFT compliance.

Compliance Officer: A management-level appointee with responsibility for day-to-day AML/CFT compliance and independent reporting.

Internal Audit or External Reviewer: Responsible for testing and auditing AML/CFT policies and controls.

5. Risk-Based Approach and Assessment

VoltEnt applies a Risk-Based Approach (RBA) to all relationships, activities, and delivery channels. A documented risk assessment is maintained and updated periodically to reflect:

- Customer profiles and geographies
- Services and delivery channels
- Nature of the business relationship
- Sanctions exposure
- Use of new products or technologies

Enhanced due diligence is applied for high-risk customers, including PEPs and cross-border entities.

6. Risk Management Measures

The Company maintains a risk-based approach to AML/CFT, which includes:

- Identifying, assessing, and understanding ML/TF risks
- Applying appropriate mitigation measures proportionate to the identified risks
- Ensuring enhanced controls are in place for higher-risk activities

7. Business Risk Assessment (BRA) and Methodology

The Company maintains a formal BRA, which:

- Assesses risks across customer profiles, jurisdictions, products/services, and delivery channels
- Uses a documented methodology combining quantitative and qualitative inputs
- Assigns risk ratings as Low, Medium, or High based on predefined criteria

8. Risk Justification and Residual Risk

The BRA outlines:

- Reasons for assigning specific risk levels
- Factors considered for residual risk levels post-mitigation
- Remaining vulnerabilities and how they are addressed

9. BRA Reassessment

The BRA is reassessed:

- Annually at minimum
- After any significant business or regulatory change
- Following identification of a major ML/TF event

10. KYC Requirements for Corporate Clients (≥ EUR 50,000)

For companies entering into agreements equal to or above ANG 100,000 / EUR 50,000, the following must be collected:

- Legal entity name, registration number, and jurisdiction
- Corporate documents (Certificate of Incorporation, Articles of Association)
- Identity of UBOs and senior management
- Source of funds and source of wealth declarations

11. KYC for Corporate Directors

Where a legal entity acts as a director, the following information is required:

- Corporate director's full registration details
- Legal representative identity and authorization documentation
- UBO details of the corporate director entity

12. Counterparty Screening

Counterparties are screened using:

- Open-source intelligence (e.g., Google searches)
- Automated AML screening tools that cover PEP, sanctions, and adverse media lists

13. Enhanced Due Diligence (EDD) for High-Risk Counterparties

EDD is triggered when a counterparty:

- Is from a FATF-listed high-risk country
- Provides false or misleading information
- Shows adverse findings in screening, EDD includes obtaining additional documentation, verifying the source of funds/wealth, and senior management approval before onboarding.

14. PEP Screening Procedure

Politically Exposed Persons (PEPs) are identified through automated screening and declaration at onboarding. Upon identification:

- Senior management approval is required
- Ongoing transaction monitoring is enhanced
- PEP status is reviewed periodically

15. Monitoring Unusual Transactions

Transactions are monitored for red flags, including:

- Identity mismatches and discrepancies
- Unusual refund requests
- Sudden changes in transaction behavior
- Involvement of high-risk jurisdictions

These transactions are reported internally and escalated to the FIU where necessary.

16. Internal Instruction (Annex 1)

The Internal Instruction on Counteracting Money Laundering and Financing of Terrorism, forming Annex 1 to this Policy, defines in detail:

- Methods of Client Identification and Verification
- Identification of Ultimate Beneficial Owners (UBOs) and PEPs
- Ongoing Monitoring and Identification of Suspicious Activity
- Record Keeping (minimum retention period: 6 years)
- Recognition and Reporting of Unusual Transactions (STRs)
- Screening Against Sanctions Lists (UN, EU, local lists)
- Staff Training and Awareness (initial and annual follow-ups)
- Independent Testing Procedures

This annex also includes definitions of key concepts and a list of applicable laws and regulations.

17. Training and Awareness

All relevant employees undergo AML/CFT training upon hiring and at least annually. The training covers:

- Company AML/CFT obligations
- Identification of ML/TF red flags
- Use of internal systems to report suspicious transactions
- Sanctions compliance requirements

18. Review and Updates

This Policy and its annexed Instruction will be reviewed at least annually or upon:

- Any change in applicable AML/CFT laws and guidelines
- A regulatory requirement or request
- Material change in the Company's risk profile or product/service offering

19. Disciplinary Measures for Non-Compliance

Failure to comply with this AML Policy, including deliberate negligence, non-reporting, or enabling unlawful financial activities, will result in disciplinary actions up to and including termination of employment, contract suspension, and/or reporting to relevant authorities.

Annexes:

Annex 1: Internal Instruction on AML/CFT Procedures (detailed operational procedures)

Annex 2: Voltent Due Diligence Form_final