

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy

Atlas Tech Solutions B.V. / pro1bet.com

Version: 1.0

Effective Date: [Insert Date]

Approved By: Executive Management

Policy Owner: AML Compliance Officer (AMLCO)

1. Introduction

Atlas Tech Solutions B.V. ("the Company"), operating the online platform pro1bet.com, is fully committed to preventing money laundering (ML), terrorist financing (TF), fraud, and all related financial crimes.

This AML/CTF Policy establishes mandatory standards, controls, and procedures designed to ensure compliance with:

- Curaçao local AML/CTF laws and regulations.
- FIU Curaçao guidance
- FATF Recommendations
- EU AML Directives (AMLD5, AMLD6), where relevant
- International sanctions frameworks (UN, EU, OFAC)

This policy applies to all Company employees, contractors, and business units involved in customer onboarding, payments, risk, operations, compliance, or financial activities.

This policy establishes the minimum AML/CTF standards to be applied across all operations and supplements local legislative requirements.

2. Legal and Regulatory Framework

The primary legislative basis includes the Landsverordening Bestrijding Witwassen en Financieringen van Terrorisme en het Financieringen van Proliferatie (National Ordinance on the Combating of Money Laundering, Terrorist Financing and Proliferation) in Curaçao.

Two important supporting ordinances:

- Landsverordening Identificatie bij Dienstverlening (LID) — the National Ordinance on Identification when Rendering Services (CGA).
- Landsverordening Melding Ongebruikelijke Transacties (LMOT) — the National Ordinance on the Reporting of Unusual Transactions (FUI & CGA).

The Curaçao Gaming Authority (CGA) (formerly/also the Gaming Control board) acts as AML/CFT supervisor in the gaming / i-gaming sector under those ordinances.

The Central Bank of Curaçao and Sint Maarten (CBCS) issues “Provisions & Guidelines on Combating Money Laundering and the Financing of Terrorism & Proliferation” for various sectors (banks, insurance, trust services, money-transfer, asset managers) in Curaçao.

Indirect CBCS Oversight via Regulated Service Providers

Although the Company does not fall under the direct prudential supervision of the Central Bank of Curaçao and Sint Maarten (CBCS) as a financial institution, it must be noted that a number of its regulated service providers – including trust offices, corporate service providers and certain financial institutions – are subject to direct supervision by the CBCS.

These service providers are required under applicable AML/CFT legislation and CBCS regulatory frameworks to perform ongoing client due diligence, transaction monitoring and risk assessments on their clients, including the Company. As part of their regulatory obligations, they must periodically report their compliance findings to the CBCS.

As a result, the Company operates under **indirect regulatory oversight** in the context of AML/CTF compliance and therefore aligns its internal controls and policies with the AML/CFT standards expected by both direct and indirect supervisory authorities.

A national strategy: the AML/CFT/CFP National Strategy and Action Plan – Curaçao (2024) (published June 4, 2024) covers Money Laundering, Terrorist Financing and Proliferation Financing (ML/TF/PF).

3. Definitions

Money Laundering: The process by which individuals or entities disguise the origins of illicit funds to make them appear legitimate.

Terrorist Financing: The act of providing financial support to individuals or groups engaged in terrorism.

Customer Due Diligence (CDD): Procedures performed to verify a customer's identity and understand the nature and purpose of the customer relationship.

Enhanced Due Diligence (EDD): Additional measures applied for higher-risk customers, jurisdictions, or transactions.

Politically Exposed Person (PEP): Individuals who hold or have held prominent public functions, including their family members and close associates.

Sanctioned Person: An individual or entity listed on recognized sanctions lists.

4. AML Governance Structure

4.1 Board of Directors & Executive Management

Responsible for ensuring the Company complies with AML obligations and allocates adequate resources.

The Board of Directors & Executive Management want to clearly express their commitment to combat the abuse of facilities and services for money laundering and the financing of terrorism and proliferation purposes.

It is the intention to comply with current anti-money laundering and terrorist financing legislation as well as the AML/CFT/CFP Provisions & Guidelines, in particular the laws and provisions regarding the identification of clients, screening of clients against sanction lists, the reporting of unusual transactions, and freezing of assets.

Atlas Tech Solutions B.V. acknowledges the importance of combating money laundering, financing of terrorism and proliferation. Money laundering, terrorist financing and/or proliferation have major economic and social consequences for businesses as well for a country. Risks range from reputational, operational, legal and financial to international sanctions, social, crime and so on.

With this Policy, enforced by the Board of Directors & Executive Management and the AMLCO, we aim to combat the possibility of any abuse of its facilities and services for money laundering and terrorist financing purposes.

Furthermore, although the Company is not directly supervised by the Central Bank of Curaçao and Sint Maarten (CBCS), it acknowledges that its regulated service providers (such as trust offices) are subject to CBCS oversight and must conduct AML/CTF compliance checks on the Company as part of their legal obligations.

The Board of Directors and Executive Management take this indirect regulatory oversight into account when designing and maintaining the Company's AML/CTF governance framework and ensure that internal compliance standards are aligned with the requirements imposed on such regulated service providers.

4.2 AML Compliance Officer (AMLCO)

The AMLCO is responsible for day-to-day AML oversight; (s)he has the role and responsibility to verify compliance of the business with respect to the detection and deterrence of money laundering and terrorist financing, and the maintaining of a sound business operation, including:

- Implementing and maintaining the AML/CTF framework
- Filing Suspicious Transaction Reports (STRs) with FIU Curaçao
- Reviewing high-risk customers and transactions
- Overseeing CDD/EDD processes
- Managing sanctions and PEP screening
- Delivering staff training

4.3 Employees

All Company's employees are required to read and apply the policies and procedures. All employees must:

- Follow the AML policy

- Conduct due diligence as required
- Report suspicious activity to the AMLCO immediately
- Maintain confidentiality regarding STR filings (“no tipping-off”)

5. Customer Due Diligence (CDD)

To manage the client’s integrity risks properly, the Company performs client due diligence. In this process, KYC is necessary and is requested from the client to verify and screen the client and understand the purpose of their business. CDD must be completed before establishing any business relationship or allowing financial activity.

5.1 Identification Requirements

For identification of a natural person, all customers must provide:

- Full name, including any aliases
- Date of birth
- Nationality
- Residential address
- Valid government-issued photo ID (passport, national ID, or driver’s license)
- Selfie photo for biometric verification

All ID images must be clear, unaltered, and show all four corners. Blurred or redacted information is not accepted.

5.2 Proof of Address (POA)

Acceptable POA documents (issued within last 3 months), can be one of the following documents:

- Utility bill
- Bank statement
- Government-issued letter
- Tax statement

5.3 Reference Letter

A reference letter issued by a reputable bank or by a Professional Intermediary. When dealing with high-risk clients (for example: PEPs), acceptance cannot be based on a single reference letter. Two reference letters are required from two different regulated financial institutions.

5.4 Verification Thresholds

As defined by FATF, having a risk-based approach means that countries, competent authorities, and banks; identifies, assesses, and understands the money laundering and terrorist financing risk to which are exposed, and take the appropriate mitigation measures in accordance with the level of risk:

Level 1 – Basic Verification (Mandatory for all customers):

- ID upload
- Selfie verification
- Basic personal data confirmation

Level 2 – Enhanced Verification (Triggered at €2,000 cumulative deposits/withdrawals):

- Full ID verification
- POA verification
- Electronic database checks

Level 3 – Source of Funds (SOF) / Source of Wealth (SOW) (Triggered at €5,000 cumulative activity):

- Bank statements
- Pay slips
- Proof of business ownership
- Tax returns

Withdrawals and deposits exceeding verification thresholds will be held until completion. Verification of the SOF/ SOW will be conducted by the AMLCO. Likewise, any funds intended to be credited, must be previously explained by the Client.

6. Enhanced Due Diligence (EDD)

Once we have the results of the Client Risk Assessment, we know which level of risk are applicable for the client and to perform the necessary enhanced client due diligence (EDD) to mitigate the client's risks accordingly.

Enhanced client due diligence entails that in addition to the minimum client due diligence which is required to perform more frequent, in depth and/or additional checks on the client. The periodic reviews for the clients are to be carried out on a yearly basis, to ensure that the client compliance file is always complete and valid.

EDD is applied, including for the following clients:

- Customers from high-risk jurisdictions (per FATF lists)
- PEPs and their associates
- Sanctioned or watch-listed individuals

- Large or unusual transactions
- Cryptocurrency-related activity

7. Risk Assessment Framework

To have a robust foundation for risk assessment and management, the risk framework of risk identification, risk analyses, risk controls and risk monitoring as the image below illustrates will be followed.

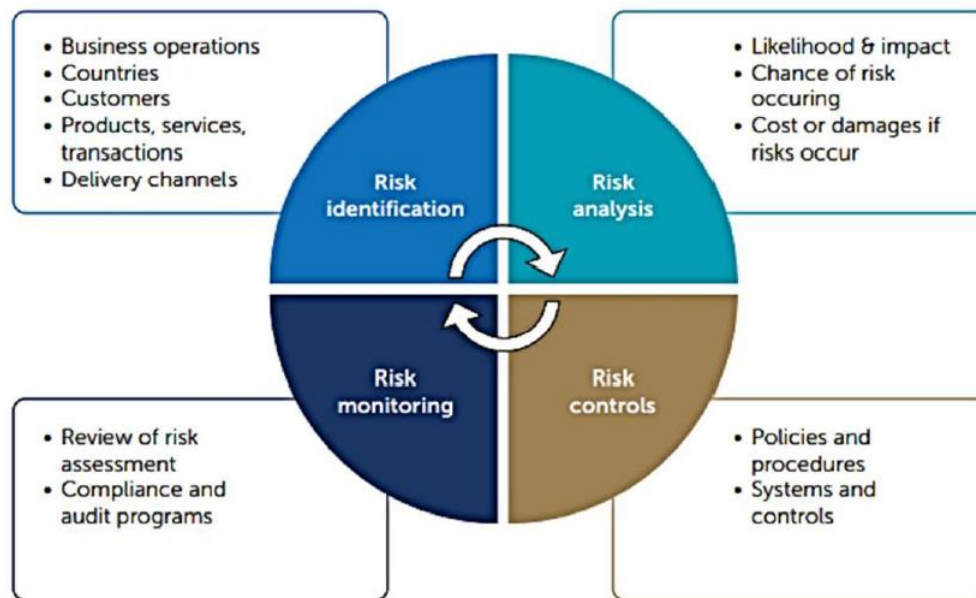


Image from CBCS guidance on the SARA

The Company maintains a systematic AML/CFT/CFP risk assessment (SARA) which will be updated annually. Risk is assessed across:

- Customer type
- Geographic location
- Transaction behavior
- Product and service risk
- Delivery channels

7.1 Country Risk Classification

Customers are categorized as:

- **Low Risk (Level 1):** Nations with strong AML controls
- **Medium Risk (Level 2):** Nations with moderate AML controls
- **High Risk (Level 3):** FATF-listed jurisdictions and sanctioned regions (Restricted)

High-risk countries may be restricted or require EDD.

8. Ongoing Monitoring

Ongoing monitoring is the continuous, risk-based review of customer activity, behaviour, and information to ensure that:

1. The customer still matches their risk profile.
2. Transactions make sense given their stated business/activity.
3. Any suspicious or unusual activity is detected and reported.
4. The customer's information stays current and accurate.

The AMLCO is responsible for ongoing monitoring of customer behaviour for unusual or suspicious activities.

8.1 Automated Monitoring

Automated monitoring refers to the use of technology-driven systems to continuously review customer activity, transactions, and behavioural patterns for potential ML/TF risks without requiring constant manual intervention. It supports the risk-based approach by allowing institutions to detect suspicious patterns in real time or near real time, especially in high-volume or high-risk industries (gaming, MSBs, fintech, online services).

Systems monitor:

- Rapid deposit–withdrawal cycles
- Mismatched payment methods
- Sudden changes in player behaviour
- Use of third-party or stolen payment instruments

8.2 Manual Review

All alerts generated by automated systems are reviewed by the AMLCO.

8.3 Prohibited Activity

Customers must withdraw using the same method used for deposits (up to deposited amount) to prevent ML layering.

9. Suspicious Transaction Reporting

Apart from hits on World Check or other screening tools when screening a transaction, an unusual transaction is a transaction that is inconsistent with the client's business activities and client financial

profile. The first key in recognizing unusual transactions is to know our client to be able to spot when something is out of the ordinary.

Transaction monitoring is a crucial part of the business and AMLCO's responsibilities, as client transactions are one of the best indicators for detecting money laundering. Employees must immediately escalate suspicious activity to the AMLCO.

The AMLCO will:

1. Investigate the activity
2. Document findings
3. Submit a Suspicious Transaction Report (STR) to FIU Curaçao when warranted
4. Maintain confidentiality and follow non-disclosure obligations

Customers must not be informed when an STR is filed.

10. Recordkeeping Requirements

All Company employees create, collect, and retain records relating to the business activities they perform. All records are handled in a manner that commensurate with our local laws and our procedures for record keeping.

The AMLCO ensures that the organizational system for the obtaining and management of records is maintained and is compliant with our local laws and legislative requirements and procedures.

The Company retains client compliance records such as client identification, account files, business correspondence, and internal and external reports related to unusual transactions.

The retention policy on our client compliance records is as follows:

- Identification documents for at least **10 years** after the customer relationship ends
- Transaction records for at least **10 years**
- STR-related logs securely and confidentially

In addition, the Company acknowledges that its AML/CTF compliance records may be requested or reviewed by regulated service providers (such as trust offices or financial institutions) in the context of their own regulatory obligations towards the Central Bank of Curaçao and Sint Maarten (CBCS). Therefore, all compliance documentation must be maintained in a structured, complete and audit-ready manner to support both internal compliance monitoring and external regulatory compliance checks conducted by such service providers.

Records are stored encrypted and protected from unauthorized access.

Our client compliance records can be divided into the following 4 areas:

- Client compliance documents;
- Client financial documents;

- Client legal documents; and
- Client tax documents.

Our minimal retention period of all records for current clients and terminated business relationships is 10 years as required by law. Furthermore, the disposal of records must first be approved by the AMLCO and Executive Management and the disposal must be in accordance with our local laws.

11. Employee Training

One important responsibility of the AMLCO is to develop or arrange for appropriate training plans/programs for the business to increase their knowledge, skills, and awareness in the field of anti-money laundering and terrorist financing. Especially the employees that are responsible for KYC and the insertion, approving or reviewing of transactions are obligated to follow an ongoing training in this field.

In addition to training, the AMLCO also periodically provides the business with memos on current AML/CFT/CFP Provisions & Guidelines topics. Or in the event the AMLCO is of opinion that the business lacks knowledge in a specific compliance topic, he/she can provide a memo to clarify that matter.

All employees involved in financial operations must receive:

- Mandatory annual AML/CTF training
- Detailed onboarding AML sessions
- Training on recognizing suspicious activity, sanctions, and PEP risks

Training completion is documented and retained.

12. Independent Audit

Yearly independent audits are performed by an outsourced auditor to test compliance with policies, procedures and controls. These tests include amongst others:

- Evaluation of the anti-money laundering and counter terrorist financing policy and procedures;
- File review of a sample of the clients to which services are provided;
- Interviews with employees who handle transactions and with their supervisors;
- Sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- Assessment of the adequacy of the record retention system.

The scope of the testing and the testing results are documented by the independent auditor, with any deficiencies/findings reported to the AMLCO and Executive Management with a request to take prompt corrective action by a certain deadline.

An external audit function will periodically review:

- AML Policy effectiveness
- Quality of CDD/EDD procedures
- Transaction monitoring systems

- Compliance with legislation

Audit reports are shared with Executive Management.

13. Data Protection

In the event of an actual or suspected data breach, the incident must be reported immediately to the AMLCO and the Executive Management.

The AMLCO shall assess the nature, scope and impact of the data breach and determine, in consultation with Executive Management and where necessary external advisors, whether notification to the competent data protection authority or other supervisory or regulatory authorities is required under applicable law.

No employee is permitted to disclose any information regarding a data breach to external parties without prior authorization from the AMLCO or Executive Management.

Where required, affected customers and relevant authorities will be informed in a timely and lawful manner, in accordance with applicable data protection regulations.

14. Policy Review and Updates

This policy is reviewed **annually** or upon regulatory changes. Updates require approval from Executive Management and the AMLCO.

15. Contact Information

For AML/CTF inquiries:

Email: amlkyc@pro1bet.com

For customer support:

Email: support-en@pro1bet.com

Approved by:

Executive Corporate Management

Andrii Iudintsev

Managing Director

