

BITEMPIRE N.V.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY

Version 1.2

Date of Approval: 21 January 2025

1. MISSION STATEMENT AND POLICY OBJECTIVES

This Anti-Money Laundering and Counter-Terrorist Financing Policy ("the Policy") sets out the strategic framework and operational standards adopted by Bitempire N.V. ("the Company") to ensure compliance with applicable anti-money laundering ("AML") and counter-terrorist financing ("CTF") legislation, regulations, and best practices. The Company is firmly committed to the global effort to prevent and detect money laundering, terrorism financing, and other forms of financial crime, and has implemented this Policy to outline its stance, define its responsibilities, and establish the procedures that are to be followed by all employees, officers, contractors, and stakeholders.

The objectives of this Policy are as follows:

- To fulfill, at all times, the statutory and regulatory obligations imposed on the Company under national and international AML and CTF legislation, with particular regard to the risks associated with the online gaming and betting sector.
- To actively and effectively mitigate the risk that the Company's operations, services, or platforms are misused as instruments for laundering the proceeds of criminal conduct or for the facilitation of terrorism or the proliferation of weapons of mass destruction.
- To avoid the establishment or continuation of business relationships with individuals or entities whose actions, conduct, or profiles give rise to a reasonable suspicion that they are involved in, or intend to engage in, unlawful or illicit activities.
- To ensure that any such suspicion or knowledge of potentially unlawful activity is promptly reported to the relevant competent authorities, in accordance with prevailing legislation, and that business relationships with such individuals or entities are terminated in a lawful, responsible, and documented manner, in coordination with such authorities.
- To uphold and adhere to all applicable national legislation in Curaçao, including, but not limited to:
 - the National Ordinance on Identification when Providing Services (NOIS),
 - the National Ordinance on the Reporting of Unusual Transactions (NORUT),
 - the Kingdom Sanctions Act and associated National Ordinances,
 - all applicable national decrees and extensions thereof,
 - and any other relevant rules or orders that may be issued from time to time by the Curaçao Gaming Control Board or equivalent regulatory authority.
- To ensure full alignment with the recommendations issued by the Financial Action Task Force (FATF), including the risk-based approach and the implementation of measures related to politically exposed persons (PEPs), beneficial ownership, customer due diligence (CDD), and record-keeping.

- To implement and maintain robust internal policies, procedures, and controls for the detection and prevention of financial crime, as well as to ensure the adequacy of employee training and internal monitoring.
- To designate a duly appointed Money Laundering Reporting Officer (“MLRO” or “Compliance officer”), who shall act as the Company’s primary point of contact with regulatory and enforcement authorities on AML/CTF matters, and who shall be responsible for:
 - receiving, documenting, and assessing internal reports of suspicious activity;
 - ensuring adequate collection and maintenance of Know Your Customer (KYC) and Know Your Business (KYB) data;
 - liaising with competent national and international agencies for the reporting of suspicious transactions;
 - remaining abreast of changes in AML regulations and risk landscapes, particularly with respect to high-risk jurisdictions;
 - developing and administering AML/CTF training and awareness programs;
 - overseeing daily compliance with AML policies and procedures;
 - responding to regulatory inquiries and inspections;
 - preparing and submitting annual AML/CTF compliance reports to the Company’s Board of Directors.

The Company’s Board of Directors, management, and employees are collectively committed to maintaining a corporate culture of integrity, transparency, and vigilance with respect to AML/CTF risks.

2. DEFINITIONS, SCOPE, AND LEGAL CONTEXT

2.1 Applicable Legal and Regulatory Instruments

This Policy is guided by and shall be interpreted in accordance with:

- Directive (EU) 2015/849 (Fourth AML Directive) on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing;
- Curaçao’s National Ordinance on the Reporting of Unusual Transactions (NORUT);
- National Ordinance on Identification when Providing Services (NOIS);
- Kingdom Sanctions Act and related implementation decrees;
- Payment Card Industry Data Security Standard (PCI DSS) v1.2;
- FATF Recommendations and international best practices.

2.2 Definitions of Money Laundering and Terrorist Financing

Money laundering refers to the process by which individuals or entities conceal the illicit origins of proceeds derived from criminal activity, thereby disguising such funds as legitimate.

The 4th AML Directive defines money laundering as comprising the following activities:

1. The conversion or transfer of property, knowing that such property is derived from criminal conduct or participation therein, for the purpose of concealing its illicit origin or assisting others in evading the legal consequences of their criminal actions;
2. The concealment or disguise of the true nature, source, location, disposition, movement, ownership, or rights pertaining to property derived from criminal activity;
3. The acquisition, possession, or use of property with knowledge, at the time of receipt, that such property has criminal origins;
4. The involvement in, facilitation of, or attempt to commit any of the aforementioned acts.

Terrorist financing involves the provision or collection of funds with the intention or knowledge that they will be used to support the commission of terrorist acts, including those set out under Articles 1 to 4 of Council Framework Decision 2002/475/JHA.

2.3 Stages of Money Laundering

Money laundering is generally understood to occur in three distinct but interrelated stages:

- **Placement:** The introduction of illicit funds into the financial system;
- **Layering:** The process of conducting complex layers of financial transactions to obscure the origin of the funds;
- **Integration:** The re-introduction of the laundered funds into the economy in a manner that appears legitimate.

3. RISK-BASED APPROACH (RBA)

The Company adopts a comprehensive risk-based approach (RBA) to AML and CTF compliance, which requires the identification, assessment, and mitigation of money laundering and terrorism financing risks in a manner that is commensurate with the nature, size, and complexity of the Company's business operations.

This approach is based on the following principles:

- Conducting periodic enterprise-wide and product-level risk assessments to identify threats and vulnerabilities.
- Categorizing customers, products, services, delivery channels, and geographic locations according to risk.
- Allocating AML resources, including due diligence procedures, according to the assessed level of risk.
- Designing and implementing policies and controls tailored to mitigate high-risk scenarios.
- Documenting and maintaining the results of all risk assessments for internal use and regulatory review.

4. GOVERNANCE, RESPONSIBILITIES, AND ACCOUNTABILITY

The responsibility for the implementation, oversight, and periodic review of this Policy rests jointly with the Company's appointed Money Laundering Reporting Officer (MLRO), the Key Official designated under applicable regulatory requirements, and other relevant senior executives, as appropriate.

4.1 Responsibilities of the MLRO and Key Official

The MLRO and Key Official shall be directly responsible for the effective administration of the Company's AML/CTF framework and shall undertake, without limitation, the following duties:

- Ensuring that all anti-fraud, KYC, and AML procedures are adhered to in accordance with regulatory expectations and internal risk appetite;
- Overseeing the operational implementation of AML systems, including the timely review of customer profiles, transaction monitoring, and risk alerts;
- Coordinating with the Chief Financial Officer (CFO) to ensure the integrity of the payout process and that disbursements are conducted only after satisfactory completion of applicable due diligence requirements;
- Maintaining an up-to-date AML/CTF policy framework and ensuring that amendments to applicable laws and guidelines are promptly reflected;
- Raising awareness and conducting regular staff training initiatives to ensure that all relevant personnel understand their obligations under this Policy;

- Serving as the Company's liaison officer with the Financial Intelligence Unit (FIU), local regulators, law enforcement, and other competent authorities.

5. CUSTOMER DUE DILIGENCE AND KNOW YOUR CUSTOMER (KYC)

The Company employs stringent Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures as part of its broader AML compliance framework. The purpose of these procedures is to verify the identity of clients, assess the risk associated with the business relationship, and monitor ongoing activity for anomalies or suspicious behavior.

5.1 Objectives of KYC Procedures

The Company's KYC policies are designed to achieve the following outcomes:

- To prevent unauthorized or ineligible persons, including minors, sanctioned individuals, or residents of restricted jurisdictions, from creating accounts or accessing Company services;
- To establish a comprehensive risk profile for each customer, taking into account geographic, behavioral, and transactional risk indicators;
- To ensure that the individual seeking to register an account is the true identity holder of the credentials submitted;
- To monitor customer behavior and transactions on an ongoing basis to detect and report potentially illicit activity;
- To identify politically exposed persons (PEPs) and individuals or entities on sanctions lists;
- To detect and block attempts to create duplicate accounts for fraudulent purposes.

5.2 Customer Registration Requirements

Prior to gaining access to the Company's gaming or transactional services, all prospective customers must complete the registration process and submit the following minimum information:

- A valid and active email address (subject to verification before any withdrawal functionality is enabled);
- A functioning mobile number;
- Full legal name;
- Date of birth;
- Current residential address.

The fraud prevention team shall perform an initial screening to identify indicators of false or misleading information, duplicate or self-excluded accounts, or matches against PEP and sanctions databases. The customer's IP address shall also be logged to detect access attempts from restricted jurisdictions. Accounts associated with such traffic may be blocked pending further review.

5.3 Age Verification

The Company does not permit individuals under the age of 18 to register or operate a user account. The system architecture enforces this prohibition by default, and identity verification tools (e.g., iDentomat) are used to confirm the customer's date of birth through valid documentation.

5.4 Duplicate Account Prevention

A customer may hold only one registered account. If system or manual checks identify the possibility of a duplicate account, the implicated account(s) shall be suspended until further investigation confirms or disproves duplication. Verified duplicate accounts will be

permanently closed. Where doubts persist about the identity or legitimacy of a customer, additional documentation will be requested, including:

- A government-issued ID (passport or national ID card);
- A credit card scan (if relevant to payment method used);
- A recent utility bill (no older than six months) evidencing current residence.

If such documentation fails to resolve the Company's concerns, the MLRO must be consulted to determine appropriate escalation.

5.5 Standard Due Diligence Triggers

The Company initiates standard due diligence procedures when any of the following circumstances arise:

- Requests to amend sensitive account details (e.g., address, email);
- Withdrawal attempts through a method different from the original deposit channel;
- Cumulative transactions (deposits or withdrawals) exceeding EUR 2,000 or NAF 4,000;
- Suspicious or unusual customer behavior;
- Questions surrounding the reliability or completeness of previously submitted identification information.

Verification may be conducted through third-party KYC tools or the collection of supporting documentation, including valid identification, proof of address, and evidence of ownership of payment method.

5.6 Enhanced Due Diligence (EDD)

Where a higher risk of money laundering or terrorist financing is identified, the Company shall initiate Enhanced Due Diligence measures. Triggers for EDD include, but are not limited to:

- Designation of the customer as a PEP or close associate of a PEP;
- Multiple accounts created under the same or similar credentials;
- IP address manipulation or shifting across jurisdictions;
- Customer is domiciled in a high-risk country or one associated with significant card fraud;
- Structured or fragmented transactions designed to evade reporting thresholds;
- Attempts to withdraw large amounts without significant gaming activity;
- Sudden deviations from historical transactional patterns;
- Customer classified as VIP or high-turnover;
- Residency or registration in a jurisdiction not included on the FATF white list.

In such cases, the customer must submit, within 30 days, a government-issued ID, utility bill, bank statement, and documentary proof of the source of funds. Failure to comply within this timeframe shall result in the account being blocked from all financial activity until such documentation is received and verified.

5.7 Record Keeping Obligations

The Company shall retain, in accordance with applicable law, all documents and records related to customer identification, due diligence, transactional history, suspicious transaction reports, training logs, and AML procedures for a minimum of five (5) years from the conclusion of the relevant transaction or the end of the business relationship. All records may be maintained in either physical or electronic format and shall be made available to the competent authorities upon request.

5.8 Politically Exposed Persons (PEPs)

A Politically Exposed Person is defined as any individual who is or has been entrusted with a prominent public function, as well as immediate family members and close associates. Given their susceptibility to corruption-related offenses, PEPs are subject to enhanced scrutiny.

Once a customer is identified as a PEP:

- Approval from senior risk management is required to establish or maintain the relationship;
- EDD procedures are conducted, including ongoing transactional monitoring;
- The customer is periodically reviewed against updated PEP lists and adverse media sources.

6. TRANSACTION MONITORING AND INTERNAL REPORTING

6.1 Identification of Suspicious Transactions

The Company has implemented both automated and manual monitoring systems to detect patterns, behaviors, and transactions that may be indicative of money laundering or terrorist financing. Red flags include, but are not limited to:

- Customer refusal to provide required identification or verification documents;
- Multiple accounts linked to the same individual;
- Use of prepaid cards for substantial deposits in a single session;
- Deposits greatly exceeding typical betting activity;
- Large withdrawal requests following minimal gaming activity;
- Frequent, unexplained deposits and withdrawals;
- Attempted fund transfers between unrelated customers or accounts;
- Discrepancies between transaction volume and known financial profile;
- Sudden shifts in gameplay behavior;
- Suspicious inquiries about transferring funds between accounts;
- Evidence of attempts to avoid AML thresholds through transaction splitting;
- Unexplained source of wealth, especially in younger or low-income individuals.

Any suspicions shall be documented and submitted to the MLRO via the prescribed Internal Suspicious Transaction Report (STR). The MLRO shall evaluate each case and determine whether external disclosure to authorities is warranted.

6.2 Prohibition of Tipping Off

All personnel are strictly prohibited from informing any customer or third party that a transaction is under investigation or has been flagged for suspicion. Such behavior constitutes “tipping off” and is a criminal offence under applicable law. Only the MLRO and essential personnel shall be informed of pending investigations. No action should be taken which might alert the subject of the investigation without prior legal or regulatory consultation.

6.3 Suspicious Employee Behavior

The same procedures applicable to customers apply equally in the event that suspicions arise regarding an employee’s conduct. Any employee suspected of engaging in, or facilitating, money laundering or terrorist financing must be reported to the MLRO via an Internal STR, with the same confidentiality protections.

6.4 Duty to Report

Failure to report a suspicious transaction, where reasonable grounds to suspect money laundering or terrorist financing exist, may itself constitute a criminal offence. All employees are reminded of their duty to report promptly and in good faith.

7. EMPLOYEE SCREENING, TRAINING, AND AWARENESS

The Company acknowledges that the effectiveness of any AML/CTF regime is dependent upon the knowledge, vigilance, and integrity of its personnel. Accordingly, the Company has adopted robust internal controls aimed at ensuring that all relevant employees are

appropriately screened, trained, and continually informed of their responsibilities under this Policy and applicable laws.

7.1 Employee Training

The Company ensures that all personnel whose roles may expose them to AML/CTF risks receive regular and comprehensive training, both at the commencement of employment and at periodic intervals thereafter. Such training shall cover, at a minimum:

- The principles and importance of customer due diligence and verification;
- Internal processes for identifying and escalating suspicious activity;
- Legal obligations concerning record keeping and the prohibition of tipping off;
- AML/CTF laws and regulations applicable to the jurisdictions in which the Company operates;
- Policies governing internal controls, risk assessment, compliance oversight, and reporting;
- The identification of behavior indicative of money laundering or terrorist financing.

Training shall be tailored to the role and level of risk exposure of each employee. The Company shall maintain detailed records of all AML/CTF training sessions, including dates, participants, content covered, and acknowledgments of completion. Competency assessments may be conducted to ensure that personnel have attained the required level of understanding.

7.2 Employee Screening and Vetting

Given the inherent risk posed by potential insider abuse, the Company shall conduct appropriate screening and background checks for all new hires in roles with AML/CTF exposure. Such checks may include:

- Verification of identity and qualifications;
- Review of previous employment and reference verification;
- Credit history and financial probity assessment;
- Criminal background screening, where permitted by law.

Employees will be subject to ongoing scrutiny during their tenure, particularly if promoted into positions of heightened responsibility or risk. The Company reserves the right to conduct follow-up assessments where deemed necessary.

To summarize, all employees in relevant roles shall be:

- Appropriately identified and verified;
- Duly vetted for integrity and competence;
- Regularly trained and tested in AML/CTF compliance.

8. MONITORING TOOLS AND TECHNOLOGICAL CONTROLS

The Company has deployed a suite of advanced technological solutions to assist in its efforts to detect, prevent, and report financial crime. These systems are designed to operate seamlessly with the Company's operational infrastructure and are configured to align with its risk appetite and compliance obligations.

8.1 Covery Solution

The Company utilizes the Covery fraud prevention platform, which provides automated decisioning based on:

- Event chain analysis;
- Feature engineering;
- Configurable rule-based scenarios;
- Real-time behavioral analytics; and

- Machine learning algorithms trained on a global dataset of fraudulent and legitimate activity.

The Covery system is configured to flag transactions or behaviors that fall outside established parameters, escalate alerts requiring human review, and reject high-risk actions as defined by internal policies.

8.2 Identomat Verification System

The Identomat platform supports the Company in conducting real-time, remote identity verification in accordance with legal requirements. Its functionality includes:

- Biometric identity checks and facial recognition;
- AML screening against international sanctions, PEP databases, and adverse media lists;
- Document authenticity verification;
- Automated onboarding for low-risk users, and manual escalation for higher-risk cases.

Both Covery and Identomat serve as integral components of the Company's defense against fraud and financial crime and are maintained in accordance with applicable data protection and security standards.

9. KNOW YOUR BUSINESS (KYB)

In addition to customer-level due diligence, the Company undertakes stringent **Know Your Business (KYB)** procedures for all third parties, counterparties, suppliers, service providers, affiliates, and other contractual business partners.

The KYB process is designed to:

- Identify and verify the legal structure, beneficial ownership, and management of any contracting entity;
- Ascertain the legitimacy and lawfulness of the business partner's operations;
- Detect any potential associations with financial crime, money laundering, terrorism financing, or other unlawful conduct.

As part of this process, the Company requires the following documentation from its business partners, prior to the commencement of any contractual relationship:

- A complete **corporate ownership chart**, detailing all entities in the holding structure up to the ultimate beneficial owner(s) (UBOs). Where ownership is held via intermediary companies, full corporate documentation must be provided for each entity.
- An **extract from the national or commercial register**, or an equivalent document, listing the company's registered address, directors, and shareholders.
- A copy of the **Memorandum and Articles of Association** or other constitutional documents.
- A valid **passport or national ID copy** for each UBO and director.
- A **utility bill or other evidence of residential address** (no older than 3 months) for each UBO and director.

The Company reserves the right to request any additional documentation or clarifications deemed necessary by the MLRO in order to complete its due diligence obligations.

10. REPORTING OF SUSPICIOUS ACTIVITY

The Company has established clear and effective internal procedures for the reporting of suspicious transactions or behavior.

10.1 Role of the MLRO

The MLRO is the primary person responsible for receiving and assessing any information which may give rise to a suspicion, or reasonable grounds for suspicion, that a person is engaged in money laundering or the financing of terrorism. The MLRO is tasked with:

- Reviewing all internal suspicious transaction reports (STRs);
- Deciding whether the matter should be disclosed to external authorities;
- Liaising with the Financial Intelligence Unit (FIU) or other competent authorities;
- Providing guidance to employees on handling suspicious situations;
- Maintaining all STR records and justifications for non-escalation decisions.

The MLRO acts independently and has unfettered access to all relevant documentation and systems necessary to carry out their duties.

10.2 Internal Reporting by Staff

All employees are under a legal and contractual duty to report any knowledge or suspicion of potential financial crime. Reports shall be made via the prescribed **Internal STR Form**, submitted directly to the MLRO. Reports must be submitted in good faith, and the reporter shall be protected from retaliation or reprisal.

10.3 Board Oversight

The Company's Board of Directors bears ultimate responsibility for the implementation and effectiveness of this Policy. The Board shall receive, at a minimum, an annual AML/CTF compliance report prepared by the MLRO. This report shall include:

- A summary of AML activities;
- An evaluation of the effectiveness of controls and procedures;
- Any material breaches or escalations;
- Recommendations for improvement.

The Board shall ensure the Company's ongoing compliance with all AML/CTF obligations and respond promptly to any lawful requests for information or audits initiated by competent authorities.



(SMES)
Solutions for Management
and Employment Support N.V.