

# ANTI-MONEY LAUNDERING & COUNTER-TERRORIST FINANCING POLICY

**MuchGaming B.V.**  
operating as Crypto.Games

|                     |                                     |
|---------------------|-------------------------------------|
| License Number      | OGI/2024/1336/1047                  |
| Licensing Authority | Curaçao Gaming Authority (CGA)      |
| Registered Entity   | MuchGaming B.V.                     |
| Platform            | Crypto.Games (crypto.games)         |
| Document Version    | 1.0                                 |
| Effective Date      | April 2026                          |
| Next Review Date    | April 2027                          |
| Approving Authority | Board of Directors, MuchGaming B.V. |
| Responsible Officer | AML Officer                         |

Prepared pursuant to the CGA AML Policy Template (January 2026)  
and GCB Regulations for Combating ML/FT/FP (January 2025)

## 1. Policy Statement

MuchGaming B.V. (hereinafter "the Company"), operating the online gaming platform Crypto.Games under license OGL/2024/1336/1047 issued by the Curaçao Gaming Authority (CGA), is fully committed to preventing its platform from being used as a vehicle for money laundering (ML), the financing of terrorism (FT), or the financing of proliferation of weapons of mass destruction (FP). This commitment is not merely a regulatory obligation — it reflects the Company's core values of integrity, transparency, and responsible operation.

This Anti-Money Laundering and Counter-Terrorist Financing Policy ("AML/CFT Policy" or "the Policy") establishes the framework within which MuchGaming B.V. identifies, assesses, mitigates, and manages the risks of money laundering, terrorist financing, and proliferation financing. The Policy applies to all operations of the Company, including all games of chance, sports betting, poker, and ancillary services offered through the Crypto.Games platform, as well as all payment methods, including cryptocurrency and fiat on-ramp solutions.

The Company adopts a risk-based approach to AML/CFT compliance, as required by the Financial Action Task Force (FATF) Recommendations and implemented through the Curaçao legal framework. This means that the Company directs its resources and controls proportionately to the areas of highest ML/FT/FP risk identified through its Business Risk Assessment and Customer Risk Assessments.

This Policy applies to all directors, officers, employees, contractors, and agents of MuchGaming B.V., without exception. All personnel are required to understand and comply with the obligations set forth herein. Non-compliance may result in disciplinary action, including termination of employment or contractual relationship, and may give rise to criminal liability.

## 2. Purpose

The purpose of this Policy is to:

- Establish a comprehensive AML/CFT/CFP compliance framework that meets all applicable legal and regulatory requirements under the laws of Curaçao and the standards of the CGA;
- Ensure that MuchGaming B.V. is not exploited by criminals seeking to launder proceeds of illegal activity or finance terrorism or proliferation through the Crypto.Games platform;
- Define the roles, responsibilities, and procedures for the identification and verification of customers (KYC), the assessment of customer risk, the monitoring of transactions, and the reporting of unusual transactions to the Financial Intelligence Unit (FIU) of Curaçao;
- Implement a structured risk-based approach to compliance that is proportionate to the ML/FT/FP risks faced by the Company;
- Provide clear guidance to all personnel on their obligations under applicable AML/CFT laws and internal procedures;
- Protect the Company, its directors, and its employees from legal, reputational, and regulatory risk associated with money laundering and terrorist financing.

This Policy has been developed in compliance with, and with reference to, the following legal and regulatory instruments:

- National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92);
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99);
- Regulation Indicators Unusual Transactions (N.G. 2015, no. 73);

- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- GCB Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (January 2025);
- CGA AML Policy Document Template for License Applicants and Holders (January 2026);
- FATF Recommendations and applicable CFATF guidance;
- National Ordinance on Games of Chance (LOK) (N.G. 2024, no. 157).

3. Audience

This Policy applies to all of the following persons and entities:

- All directors and officers of MuchGaming B.V.;
- All employees of the Company, irrespective of their role, seniority, or location;
- All contractors, consultants, and temporary staff who perform functions on behalf of the Company;
- All agents and third parties to whom elements of AML/CFT compliance functions have been delegated or outsourced, to the extent that such delegation is permitted under applicable law;
- All subsidiaries and affiliates of MuchGaming B.V. that are subject to the Company's compliance oversight.

All persons within the scope of this Policy are expected to familiarise themselves with its content and comply with the obligations applicable to their role. The AML Officer is responsible for ensuring that this Policy is effectively communicated and implemented throughout the organisation.

4. Definitions

The following terms, as used in this Policy, shall have the meanings set out below:

| Term    | Definition                                                                                                                                                                                                             |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AML/CFT | Anti-Money Laundering and Counter-Terrorist Financing.                                                                                                                                                                 |
| BRA     | Business Risk Assessment — a documented assessment of the ML/FT/FP risks to which the Company is exposed as a result of its business activities, customer base, products, delivery channels, and geographic footprint. |
| CAP     | Customer Acceptance Policy — the policy that sets out the conditions under which the Company will or will not establish or maintain a business relationship with a customer, based on the customer's risk profile.     |
| CDD     | Customer Due Diligence — the process of identifying and verifying the identity of a customer, understanding the purpose and nature of the business relationship, and conducting ongoing monitoring.                    |

| Term                             | Definition                                                                                                                                                                                    |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CFATF</b>                     | Caribbean Financial Action Taskforce — the regional AML/CFT body of which Curaçao is a member.                                                                                                |
| <b>CGA</b>                       | Curaçao Gaming Authority — the regulatory authority responsible for issuing and supervising online gaming licenses in Curaçao.                                                                |
| <b>AML Officer</b>               | AML Officer — the senior officer designated by the Company to oversee the AML/CFT compliance program.                                                                                         |
| <b>CRA</b>                       | Customer Risk Assessment — an individual assessment of the ML/FT/FP risk posed by a specific customer based on their identity, activity profile, geographic location, and other risk factors. |
| <b>EDD</b>                       | Enhanced Due Diligence — heightened CDD measures applied to customers who present a higher risk of ML/FT/FP.                                                                                  |
| <b>FATF</b>                      | Financial Action Task Force — the international standard-setting body for AML/CFT, whose 40 Recommendations form the basis of Curaçao's legal framework.                                      |
| <b>FIU</b>                       | Financial Intelligence Unit Curaçao — the competent authority responsible for receiving, analysing, and disseminating unusual transaction reports.                                            |
| <b>FP</b>                        | Financing of Proliferation — the provision of funds or services for the manufacture, acquisition, or transfer of weapons of mass destruction.                                                 |
| <b>FT / TF</b>                   | Financing of Terrorism / Terrorist Financing.                                                                                                                                                 |
| <b>GCB</b>                       | Curaçao Gaming Control Board — the supervisory authority for AML/CFT compliance in the Curaçao gaming sector.                                                                                 |
| <b>KYC</b>                       | Know Your Customer — the overall process of identifying and verifying the identity of customers.                                                                                              |
| <b>ML</b>                        | Money Laundering — the process of concealing the origins of illegally obtained funds to make them appear legitimate.                                                                          |
| <b>XCG.</b>                      | Netherlands Antillean Florin — the currency in which statutory thresholds under Curaçao AML law are expressed.                                                                                |
| <b>NOIS</b>                      | National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92).                                                                                                  |
| <b>NORUT</b>                     | National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99).                                                                                                              |
| <b>PEP</b>                       | Politically Exposed Person — an individual who is or has been entrusted with a prominent public function, and their close family members and associates.                                      |
| <b>Risk-Based Approach (RBA)</b> | An approach whereby the Company identifies, assesses, and understands its ML/FT/FP risks and applies measures proportionate to those risks.                                                   |
| <b>SDD</b>                       | Simplified Due Diligence — reduced CDD measures applicable where the risk of ML/FT is demonstrably lower.                                                                                     |

| Term                            | Definition                                                                                                                                                                               |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source of Funds                 | The origin of the funds used for a particular transaction (e.g., employment income, savings, gambling winnings).                                                                         |
| Source of Wealth                | The origin of the customer's total wealth accumulated over their lifetime (e.g., business income, inheritance, investments).                                                             |
| UBO / Beneficial Owner          | The natural person(s) who ultimately own(s) or control(s) the customer, or on whose behalf a transaction is conducted.                                                                   |
| UTR                             | Unusual Transaction Report — a report filed with the FIU Curaçao pursuant to the NORUT.                                                                                                  |
| Virtual Assets / Cryptocurrency | Digital representations of value that can be digitally traded or transferred, including Bitcoin (BTC), Ethereum (ETH), and other cryptocurrencies accepted on the Crypto.Games platform. |

## 5. Policy Implementation

The following sections describe how this Policy is implemented across the Company's operations. The AML Officer has day-to-day responsibility for overseeing all aspects of implementation and for ensuring that the controls described herein are functioning effectively.

### 5.1 Business Risk Assessment (BRA)

#### 5.1.1 Purpose and Scope

MuchGaming B.V. conducts a formal Business Risk Assessment (BRA) to identify, understand, and document the ML/FT/FP risks to which the Company is exposed by virtue of its business model, customer base, products and services, delivery channels, and geographic reach. The BRA forms the foundation of the Company's risk-based approach and informs the design and calibration of all AML/CFT controls.

#### 5.1.2 Risk Factors Assessed

The BRA considers the following categories of risk:

- Customer risk: The risk arising from the type of players served by the platform, including high-volume players, players from high-risk jurisdictions, players using anonymous payment methods, and any players exhibiting unusual behavioral patterns.
- Geographic risk: The risk associated with the jurisdictions from which the Company's players originate, or to which funds may flow, taking into account FATF blacklists and grey lists, CFATF public statements, OFAC designations, Transparency International Corruption Perceptions Index, and other authoritative sources.
- Product and service risk: The risks inherent in the Company's specific product offerings, including provably fair games, sports betting, poker, and cryptocurrency-based payment solutions. Of particular relevance is the anonymous nature of many cryptocurrency transactions, the use of multiple wallets, peer-to-peer transfers, and the potential for wash-trading.
- Delivery channel risk: The risk arising from the fully online, non-face-to-face nature of the Company's business, which increases exposure to identity fraud and impersonation risk. The use of third-party on-ramp providers and blockchain analytics integrations is considered in this context.

- Technological risk: The risks arising from the use of new or developing technologies, including blockchain-based payment rails, decentralised finance integrations, and automated KYC verification systems.

### **5.1.3 Outcome and Risk Appetite**

The BRA produces a documented risk profile for the Company, identifying areas of low, medium, and high ML/FT/FP risk. On the basis of this assessment, the Board of Directors sets the Company's risk appetite — that is, the level of residual risk the Company is prepared to accept after controls are applied. The Company's risk appetite is conservative: the Company will not knowingly maintain business relationships with customers who present an unacceptably high and unmitigable risk of ML/FT/FP.

### **5.1.4 Technological Development Risk Assessment**

Prior to the launch of any new product, business practice, delivery mechanism, or technology — including new cryptocurrency integrations or new payment providers — the Company conducts a specific technological development risk assessment to determine whether the innovation creates a vulnerability that could be exploited for ML/FT. Such assessments are documented and must be approved by the AML Officer before the new product or technology is deployed.

### **5.1.5 Review and Approval**

The BRA is reviewed and updated whenever material changes occur to the Company's operating environment, including the introduction of new games, new payment methods, new markets, or changes in regulatory requirements. In the absence of such changes, the BRA is reviewed at least annually. The BRA must be documented, approved by the Board of Directors, and made available to the GCB and CGA upon request.

## **5.2 Customer Risk Assessment (CRA)**

### **5.2.1 Purpose**

A Customer Risk Assessment (CRA) is conducted in respect of each player to determine the ML/FT/FP risk that the specific business relationship poses to the Company. The CRA enables the Company to categorise each customer as low, medium, or high risk, and to apply the appropriate level of Customer Due Diligence accordingly.

### **5.2.2 Timing**

The CRA is conducted at the time of establishing the business relationship — that is, at the point at which the player opens an account — and is updated as additional information is collected, or when circumstances change. A provisional risk rating is assigned based on the minimum identification information collected at registration; this rating is revised once the XCG. 4,000 threshold is reached and full CDD is conducted.

### **5.2.3 Risk Factors Considered**

The CRA takes into account the following factors:

- The player's nationality, country of residence, and country of birth, with reference to the Company's list of high-risk jurisdictions;
- The player's PEP status and sanctions screening results;
- The player's declared source of funds and, where applicable, source of wealth;
- The payment methods used by the player, including the type and origin of cryptocurrency wallets;
- The player's expected level and pattern of activity, based on declared information and — where the customer base is sufficiently large — statistical benchmarking;
- Any adverse media, negative news, or other derogatory information identified through screening;

- Indicators of unusual or suspicious behavior observed at or after onboarding.

#### **5.2.4 Risk Categories**

Based on the CRA, each customer is assigned one of the following risk categories:

- Low Risk: Customers presenting no elevated risk factors, from low-risk jurisdictions, using standard payment methods, with a consistent and expected activity pattern. Standard CDD applies.
- Medium Risk: Customers presenting some elevated risk factors that do not individually trigger EDD but that, in combination, indicate a need for closer attention. Standard CDD with enhanced monitoring applies.
- High Risk: Customers who meet one or more criteria for EDD, including PEP status, origin from a high-risk jurisdiction, use of anonymous payment methods, unexplained high-value activity, or adverse media findings. Enhanced Due Diligence applies.

### **5.3 Customer Acceptance Policy (CAP)**

#### **5.3.1 General Principles**

MuchGaming B.V. will not establish or maintain a business relationship with any customer where doing so would violate applicable law, create an unacceptable ML/FT/FP risk, or breach the terms of the Company's gaming license. The Customer Acceptance Policy sets out the conditions under which the Company will accept, reject, or restrict a player's account.

#### **5.3.2 Permitted Customers**

The Company may establish a business relationship with any individual who:

- Is aged 18 or above (verified through KYC documentation);
- Does not reside in or originate from a Restricted Jurisdiction (as defined by the Company's list of prohibited countries);
- Is not listed on any applicable sanctions list (UN, EU, OFAC, or local Curaçao designations);
- Has provided, or is in the process of providing, the minimum identification information required by this Policy;
- Has accepted the Company's Terms of Service.

#### **5.3.3 Higher-Risk Customers**

The following categories of customers are considered to present a higher than average risk of ML/FT/FP and are subject to Enhanced Due Diligence prior to or upon reaching the XCG. 4,000 threshold:

- Politically Exposed Persons (PEPs) and their family members and close associates;
- Customers from countries on the FATF list of High-Risk Jurisdictions subject to a Call for Action or Jurisdictions under Increased Monitoring;
- Customers using anonymous or high-risk payment methods, including unregulated or unlicensed e-wallets, pre-paid cards, or privacy-focused cryptocurrencies;
- Customers exhibiting high-volume or high-frequency deposit and withdrawal patterns inconsistent with their declared profile;
- Customers who have previously been flagged for suspicious activity or have been the subject of an unusual transaction report;
- Customers whose source of funds or source of wealth cannot be satisfactorily established;

- Customers who deposit and withdraw without meaningful engagement in gameplay (i.e., minimal wagering relative to deposit/withdrawal volumes);
- Customers using multiple accounts, multiple wallets, or funding patterns that appear designed to structure transactions below reporting thresholds.

### **5.3.4 Prohibited Customers — Grounds for Refusal or Termination**

The Company will decline to establish, or will terminate, a business relationship in any of the following circumstances:

- The customer is a natural or legal person listed on any applicable sanctions list;
- The customer is resident in or originates from a jurisdiction subject to comprehensive sanctions (including but not limited to Iran, North Korea, Russia in respect of sanctioned activities, Syria, and Cuba);
- The customer is unable or unwilling to provide the required identification and CDD documentation within the prescribed timeframes;
- The customer's CDD information is inconsistent, implausible, or cannot be verified;
- The Company has reasonable grounds to suspect that the business relationship is being used for ML/FT/FP;
- The customer has provided false or fraudulent identity information;
- The customer is a minor (under 18 years of age);
- Maintaining the business relationship would violate any applicable law or regulatory requirement.

### **5.3.5 PEP-Specific Requirements**

No business relationship with a PEP may be established or continued without the prior approval of senior management (or the AML Officer on behalf of senior management). Senior management approval must be documented in writing. Where a player is identified as a PEP, enhanced ongoing monitoring is applied and source of wealth information must be obtained and verified.

## **5.4 Customer Due Diligence (CDD)**

### **5.4.1 Obligation to Apply CDD**

MuchGaming B.V. is required to apply CDD measures in the following circumstances:

- When establishing a business relationship (i.e., when a player registers an account);
- When financial transactions (deposits or withdrawals) reach or exceed the equivalent of XCG. 4,000;
- When there is a suspicion of ML/FT/FP, regardless of transaction value;
- When the Company has doubts about the veracity or adequacy of previously collected identification information.

For the purposes of calculating the XCG. 4,000 threshold, all deposits and withdrawals made by the player since the establishment of the business relationship are cumulated on a daily basis, including peer-to-peer transfers. Once the threshold is reached, the full suite of CDD measures described below must be completed.

### **5.4.2 Minimum Identification at Registration**

Upon registration, and before any deposit is permitted, the Company collects the following minimum identification information from each player:

- Full name (first name and surname);

- Permanent residential address;
- Date of birth;
- Email address.

In addition, PEP status screening and sanctions screening are conducted at the point of registration in respect of all players.

#### **5.4.3 Full CDD Measures**

Upon reaching the XCG. 4,000 threshold, the Company applies the full suite of CDD measures, which consist of the following elements:

- Identification of the player: Collection of full identifying information, including full name, permanent residential address, date of birth, place of birth, nationality, and identity number;
- Verification of the player's identity: Verification of the player's identity using a valid, unexpired, government-issued photographic identity document (passport or national identity card). Proof of address must also be verified using a bank statement, utility bill, or official letter not more than six months old. Additional verification methods may include biometric checks, verification codes, geo-location cross-referencing, and IP address analysis;
- Identification and verification of the beneficial owner: The Company requires all players to register accounts exclusively on their own behalf. Players must explicitly accept a declaration to this effect in the Terms of Service. The Company's ongoing monitoring procedures include controls to detect instances where a player may be acting on behalf of third parties. Where beneficial ownership by third parties is identified, those persons must also be identified and verified;
- Understanding the purpose and intended nature of the business relationship: The Company develops a risk profile for each customer that establishes their expected level and pattern of activity. At lower risk levels, a declaration from the customer regarding their source of funds and approximate income may be sufficient. At higher risk levels, independent and documentary verification of source of funds and source of wealth is required;
- PEP status screening and sanctions screening: All players are screened against UN and EU sanctions lists and checked for PEP status at the time of reaching the threshold. Screening is conducted using automated tools and supplemented by internet searches and specialist databases where appropriate.

#### **5.4.4 Restriction of Account Activity Pending CDD Completion**

Once the XCG. 4,000 threshold is triggered by a deposit, the player may not make further deposits or withdrawals until CDD is completed. The player may continue to use funds already in their account. If the threshold is triggered by a withdrawal request, the account is fully frozen pending CDD completion, and the player may not continue playing.

#### **5.4.5 Failure to Provide CDD Documentation**

If the player fails to provide the requested CDD documentation and information within 30 calendar days of the threshold being reached, the Company will terminate the business relationship. The account will be closed or blocked. Where no presumption of ML/FT/FP exists, funds will be returned to the same source from which they were deposited (same wallet address or bank account). Where a presumption of ML/FT/FP exists, an unusual transaction report will be filed with the FIU, and the funds will be held pending further guidance from competent authorities, taking into account the risk of tipping off the player.

#### **5.4.6 Enhanced Due Diligence (EDD)**

Enhanced Due Diligence is applied to all customers classified as high risk, and in any of the following circumstances:

- The customer is a PEP or a family member or close associate of a PEP;
- The customer is resident in or originates from a high-risk jurisdiction;
- The customer is using a payment method that presents a higher risk of ML/FT;
- The customer's transaction patterns deviate significantly from their declared profile;
- The customer is using anonymous payment technologies or privacy-focused cryptocurrencies.

EDD measures include, as appropriate:

- Obtaining additional identification documents and verifying additional personal details;
- Obtaining and independently verifying source of funds and source of wealth information;
- Obtaining senior management approval to establish or continue the business relationship;
- Conducting enhanced and more frequent ongoing monitoring;
- Obtaining information on the reasons for unusual or high-value transactions;
- Requiring the first payment to be made from an account held in a reputable jurisdiction.

#### **5.4.7 Simplified Due Diligence (SDD)**

Simplified Due Diligence may be applied where the ML/FT/FP risk is demonstrably low, taking into account the customer's risk profile and the context of the business relationship. SDD is never permissible where there is a suspicion of ML/FT/FP. In the context of Crypto.Games, SDD is limited in its application given the platform's cryptocurrency focus and non-face-to-face nature, both of which are risk-elevating factors. The AML Officer must specifically authorise the application of SDD in any case.

#### **5.4.8 Politically Exposed Persons (PEPs)**

For all PEPs, whether identified at onboarding or during the business relationship, the Company applies the following requirements in addition to standard CDD:

- A risk-based system for identifying PEP status at onboarding and through ongoing screening;
- Written senior management approval (or AML Officer approval) before establishing or continuing the business relationship;
- Reasonable measures to establish and verify the PEP's source of wealth and source of funds, using independent and reliable sources (public records, media, official databases);
- Enhanced ongoing monitoring of the PEP's account activity and transactions.

The PEP requirements apply to domestic and foreign PEPs, persons entrusted with prominent functions by international organisations, and their family members and known close associates. Screening for PEP status is conducted at onboarding and at regular intervals during the business relationship. If a player who was not previously identified as a PEP becomes one, the Company must implement the relevant EDD measures within 30 days of identification.

#### **5.4.9 Ongoing Sanctions Screening**

All players are screened against UN and EU consolidated sanctions lists at the point of onboarding. Ongoing sanctions screening is conducted in real time or at regular intervals using automated screening tools that are updated whenever the relevant sanctions lists are amended. The Company monitors updates to GCB-published sanctions decrees and regulations, and updates its procedures accordingly.

If a player is identified as a sanctioned person or entity during the business relationship, the Company will immediately freeze the relevant account and any associated funds, file a report with the FIU Curaçao, and take no further action with respect to the frozen funds without guidance from competent authorities. Sanctions decrees and their amendments are monitored through the GCB website.

#### **5.4.10 CDD for Existing Customers**

The Company applies CDD measures to existing customers on a risk-sensitive basis and at appropriate intervals. Where legacy customer records are incomplete, the Company conducts remediation CDD, prioritising the highest-risk customers first. Trigger events for refreshing CDD on existing customers include changes to payment instruments, significant changes in transaction patterns, expiry of identity documents, or the emergence of adverse information.

### **5.5 Ongoing Monitoring**

#### **5.5.1 Purpose**

Ongoing monitoring is a core element of the Company's CDD program. It encompasses both the monitoring of customer identity information (to ensure it remains accurate and current) and the monitoring of transactions and account activity (to detect unusual or suspicious behavior).

#### **5.5.2 Monitoring of Customer Identity**

The Company maintains accurate and up-to-date identification data for all customers. The AML Officer ensures that systems are in place to detect changes in customer identity information, to track the expiry dates of identity documents, and to refresh identity records on a risk-sensitive basis. Significant changes — such as a change of payment method, a change of address, or a change in nationality — trigger a reassessment of the customer's risk profile.

#### **5.5.3 Transaction Monitoring**

The Company employs automated transaction monitoring tools to scrutinise customer account activity on an ongoing basis. The monitoring system is designed to detect the following indicators, among others:

- Deposits and withdrawals that are disproportionate to the player's declared income or expected activity profile;
- Frequent deposits followed immediately by withdrawals with minimal gameplay;
- Structuring of transactions to remain below the XCG. 4,000 CDD threshold or the XCG. 5,000 reporting threshold;
- Use of multiple cryptocurrency wallets or frequent changes to funding methods;
- Transfers of funds between gaming accounts;
- Peer-to-peer transfers inconsistent with a player's gaming profile;
- Activity patterns consistent with the layering or integration phases of money laundering;
- Use of blockchain addresses associated with sanctioned persons, mixers, or high-risk exchanges (as identified through blockchain analytics tools);
- Sudden and unexplained increases in deposit frequency or volume;
- Activity from IP addresses or locations inconsistent with the player's declared jurisdiction.

Where the monitoring system identifies a potential anomaly, the relevant alert is reviewed by the compliance team. If the review confirms that the transaction or pattern of activity is unusual, the matter is escalated to the AML Officer for determination of whether a UTR should be filed with the FIU. The level of monitoring applied to each customer is calibrated to their risk rating — enhanced monitoring is applied to high-risk customers, while standard monitoring applies to low-risk customers.

#### **5.5.4 Blockchain Analytics**

Given the cryptocurrency-focused nature of the Crypto.Games platform, the Company uses blockchain analytics tools to assess the risk profile of incoming and outgoing transactions. These tools are used to identify wallet addresses associated with sanctioned entities, known illicit actors, mixers, peer-to-peer exchanges, and other high-risk counterparties. Blockchain analytics findings are incorporated into the customer's risk profile and may trigger EDD or UTR filing.

## **5.6 Reliance on Third Parties to Perform Customer Due Diligence**

### **5.6.1 Permitted Third-Party Reliance**

MuchGaming B.V. may, in limited circumstances and subject to the conditions set out below, rely on third parties to perform elements (a) through (c) of the CDD measures described in Section 5.4 (identification of the customer, identification of the beneficial owner, and understanding the purpose and nature of the business relationship). Such reliance does not absolve the Company of ultimate responsibility for CDD compliance.

### **5.6.2 Conditions for Third-Party Reliance**

Reliance on a third party is permissible only where all of the following conditions are met:

- The Company obtains the relevant CDD information from the third party immediately;
- The Company has a written agreement with the third party stipulating that copies of identification data and CDD documentation will be made available to the Company upon request, and this arrangement is tested regularly to confirm it operates as intended;
- The third party is regulated, supervised, or monitored for compliance with CDD and record-keeping requirements equivalent to those applicable in Curaçao;
- The third party is not based in a high-risk jurisdiction, as assessed by reference to the Company's geographic risk framework;
- The Company is satisfied as to the reliability and integrity of the third party's CDD procedures.

### **5.6.3 Retained Responsibilities**

Regardless of any third-party reliance arrangement, the Company retains sole responsibility for conducting the CRA, determining PEP status, and conducting ongoing monitoring. The decision whether to onboard a customer, or to continue or terminate a business relationship on the basis of ML/FT/FP risk, may not be delegated to any third party.

### **5.6.4 Outsourcing and Agents**

Where elements of the AML/CFT program are outsourced to external service providers or performed by agents (for example, KYC identity verification providers), such arrangements are governed by formal written contracts that set out the provider's obligations. The Company conducts periodic assessments of the service provider's performance, both quantitatively and qualitatively. Any customer onboarded through an agent or service provider is subject to the same checks and controls as customers onboarded directly by the Company. The Company remains responsible for the acts and omissions of all agents and service providers with respect to AML/CFT compliance.

## **5.7 Reporting of Unusual Transactions**

### **5.7.1 Recognition of Unusual Transactions**

The Company has established procedures for recognising unusual transactions based on the objective and subjective indicators set out in the Regulation Indicators Unusual Transactions (N.G. 2015, no. 73). All employees who handle transactions or customer accounts receive training on recognising these indicators.

The following transactions are deemed unusual and must be reported to the AML Officer for assessment:

- Any transaction that has been reported to the Police or the Department of Justice in connection with ML or TF;
- Any transaction by or on behalf of a person or entity listed on a sanctions list adopted pursuant to the Sanctions National Ordinance;
- Any financial transaction (individual or cumulative within a gaming day) with a value equivalent to XCG. 5,000 or more, including cashless transfers, deposits, chip sales, and cash-outs;
- Any transaction where there is a reasonable basis to suspect that it may relate to ML or TF.

Note: A transaction includes any single transaction, or a series, combination, or pattern of transactions totalling XCG. 5,000 or more within a gaming day.

### **5.7.2 Internal Reporting Procedure**

All employees who identify an unusual transaction or behavior are required to report this immediately to the AML Officer (or a designated deputy) using the Company's internal unusual transaction reporting form. The report must be accompanied by all available supporting documentation, including copies of identification documents, account statements, and transaction records.

The AML Officer reviews all internal reports for completeness and accuracy. Where the AML Officer determines that the transaction meets the criteria for external reporting, a UTR is prepared and submitted to the FIU without delay. Where the AML Officer determines that external reporting is not required, the reasons for that determination are documented and signed off by the AML Officer.

### **5.7.3 External Reporting to the FIU**

MuchGaming B.V. is registered with the FIU Curaçao and has access to the goAML reporting portal. All external unusual transaction reports are filed through the goAML portal in accordance with the FIU's reporting requirements. Reports and supporting documentation are submitted in English.

The Company files UTRs without delay upon determining that a transaction is unusual. There is no minimum review period before filing — where the AML Officer is satisfied that reporting is required, the report is filed immediately.

The Company and its directors, officers, and employees are protected by law from civil and criminal liability for breach of any restriction on disclosure of information when reporting in good faith to the FIU.

### **5.7.4 Prohibition of Disclosure (Tipping Off)**

The Company, its directors, officers, and employees are strictly prohibited from disclosing to any customer, or to any third party, that an unusual transaction report has been filed with the FIU, or that the FIU has requested information. This prohibition applies absolutely and without exception.

In circumstances where a UTR has been or is being filed, the Company exercises caution in taking any action that might alert the player to the fact that a report is being made. Where the Company is required to take action such as account restriction or termination, it considers carefully whether doing so would constitute an unlawful disclosure. Where doubt exists, the preferred approach is to increase monitoring and file additional reports rather than to take drastic account action.

### **5.7.5 Record Keeping**

The Company maintains records of all transactions, CDD information, and unusual transaction reports for a minimum of five years from the date of the transaction or the end of the business relationship, whichever is the later. This is consistent with the requirements of the NOIS and NORUT. In practice, the Company applies a retention period of ten years in accordance with its Operational Manual.

Records must be maintained in a form that permits the reconstruction of individual transactions, including the amounts involved, the currencies used, the payment methods, and the wallet addresses. All records are available to the GCB, CGA, FIU, and other competent authorities upon appropriate legal request.

## **5.8 Anti-Money Laundering Compliance Program**

### **5.8.1 Overview**

The Company's AML/CFT compliance program is designed to ensure that all applicable legal obligations are met, that ML/FT/FP risks are effectively managed, and that the Company's systems and controls are subject to continuous monitoring and improvement. The program consists of four core elements:

- A system of internal policies, procedures, and controls;
- The appointment of a dedicated Compliance Officer with day-to-day oversight of the program;
- An employee screening program and an ongoing employee training program;
- An independent audit function to test the effectiveness of the program.

### **5.8.2 Internal Policies, Procedures, and Controls**

This AML/CFT Policy constitutes the primary policy document of the Company's compliance program. It is supplemented by detailed operational procedures and internal controls maintained by the AML Officer. These procedures translate this Policy into day-to-day practice and address, among other things, the step-by-step process for onboarding customers, the specific triggers and procedures for CDD and EDD, the process for filing UTRs, the procedures for account restriction and termination, and the internal escalation framework.

All policies and procedures are maintained in writing, are approved by the Board of Directors, and are communicated to all relevant employees. The AML Officer is responsible for maintaining a process to track regulatory changes and update the compliance program accordingly.

### **5.8.3 The AML Officer**

MuchGaming B.V. has designated an AML Officer responsible for the day-to-day handling of unusual transaction reports and related record-keeping.

The AML Officer's responsibilities are:

- Reviewing all internally reported unusual transactions for completeness and accuracy;
- Maintaining records of internally and externally reported unusual transactions;
- Preparing and filing external UTRs with the FIU;

### **5.8.4 Employee Screening**

The Company conducts criminal background checks on all employees prior to engagement, and periodically thereafter. No individual with a criminal conviction for ML/FT, fraud, or a predicate offence may be employed in a function with access to customer financial data or compliance functions. Employment candidates for compliance roles are subject to enhanced vetting. The AML Officer maintains records of all employee screening outcomes.

### **5.8.5 Employee Training**

The Company provides AML/CFT training to all employees whose roles may involve exposure to ML/FT/FP risks. Training is mandatory for all new employees before they begin handling customer transactions or accounts, and is refreshed at regular intervals (at minimum annually) to reflect current ML/FT typologies, regulatory changes, and the Company's own risk experience.

Training is tailored to the employee's role and covers, at a minimum, the following topics:

- The nature and process of money laundering, terrorist financing, and proliferation financing;
- The legal framework applicable in Curaçao, including the NOIS, NORUT, Sanctions National Ordinance, and Kingdom Sanction Act;
- The Company's AML/CFT policies and procedures;
- Customer due diligence requirements and procedures;
- Objective and subjective indicators for unusual transactions;
- The internal and external reporting obligations of employees;
- The prohibition on tipping off;
- ML/FT methods and typologies specific to the online gambling and cryptocurrency sectors.

Records of all training provided, including content, dates, attendees, and testing outcomes, are maintained by the AML Officer for a minimum of five years.

### **5.8.6 Independent Audit**

The Company's AML/CFT compliance program is subject to independent audit at least annually. The audit may be conducted by an adequately resourced internal audit function or by an external independent party. The auditors must be free from any involvement in the Company's compliance operations and must have appropriate qualifications, including at minimum two years of experience in AML/CFT compliance and a relevant certification (such as CAMS or AMLFC).

The annual AML audit must encompass, at minimum:

- A review of the completeness and adequacy of the Company's AML/CFT policies and procedures;
- An assessment of compliance management and the effectiveness of the AML Officer function;
- Transaction testing, including a review of a sample of unusual transactions above and below the reporting threshold;
- An assessment of the adequacy of employee training;
- An assessment of compliance with applicable laws and regulations;
- Interviews with employees who handle transactions and their supervisors;
- An assessment of the record retention system;
- A review of remediation actions from prior audits.

The results of the audit, including any deficiencies identified, are reported to senior management and the Board of Directors (or Board of Supervisory Directors) with a requirement to implement corrective actions by a specified deadline. Corrective actions, and their implementation, are tracked by the AML Officer.

## **6. Compliance and Consequences of Non-Compliance**

Compliance with this Policy is mandatory for all persons within its scope. The Company takes seriously any breach of its AML/CFT obligations and will respond proportionately to any identified failure.

### **6.1 Internal Consequences**

Failure by any employee or contractor to comply with the requirements of this Policy may result in:

- Formal written warning;
- Suspension from duties pending investigation;
- Termination of employment or contractual relationship;

- Referral to competent authorities where the breach constitutes a criminal offence.

## 6.2 Legal and Regulatory Consequences

Non-compliance with applicable AML/CFT law exposes the Company and its officers and employees to:

- Administrative sanctions by the GCB or CGA, including fines, license suspension, or license revocation;
- Criminal prosecution under the Code of Criminal Law of Curaçao (N.G. 2011, no. 48) for participation in or facilitation of money laundering, terrorist financing, or proliferation financing;
- Civil liability for losses caused to third parties as a result of AML/CFT failures;
- Reputational damage to the Company and its officers.

## 6.3 Reporting Obligations of Employees

Any employee who becomes aware of a potential breach of this Policy, or of any suspicious activity that has not been properly reported, is required to raise the matter immediately with the AML Officer. The Company does not tolerate any form of retaliation against employees who make good-faith reports of potential AML/CFT breaches. Employees who report concerns in good faith are protected from disciplinary action.

## 7. Related Information

This Policy should be read in conjunction with the following internal and external documents:

### 7.1 Internal Policies and Procedures

- MuchGaming B.V. Operational Manual (Version 1.0, April 2026);
- Privacy Policy — Crypto.Games;
- Terms of Service — Crypto.Games;
- Responsible Gaming Policy — Crypto.Games;
- Self-Exclusion Policy — Crypto.Games;
- Dispute Resolution Policy — Crypto.Games;
- Code of Conduct — Crypto.Games;
- Fairness Statement — Crypto.Games;
- AML/CFT Statement — Crypto.Games (Version 2.0, December 2025).

### 7.2 Regulatory Framework

- GCB Regulations for Combating Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (January 2025);
- CGA AML Policy Document Template for License Applicants and Holders (January 2026);
- National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92);
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99);
- Regulation Indicators Unusual Transactions (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Ordinance on Games of Chance (LOK) (N.G. 2024, no. 157);

- FATF 40 Recommendations;
- Code of Criminal Law (Penal Code) of Curaçao (N.G. 2011, no. 48).

7.3 Useful References and Databases

- UN Sanctions List: <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>
- EU Sanctions Map: <http://www.sanctionsmap.eu/#/main>
- FATF High-Risk Jurisdictions: <https://www.fatf-gafi.org>
- GCB Website (Sanctions Updates): <https://www.gamingcontrolcuracao.org>
- Transparency International Corruption Perceptions Index: <https://www.transparency.org>
- Know Your Country: <https://www.knowyourcountry.com>
- PEP Caribbean List (available via specialist compliance databases)

8. Contact Information

For any questions regarding this Policy, or to report a potential AML/CFT concern, please contact:

|                    |                                                         |
|--------------------|---------------------------------------------------------|
| Name / Role        | AML Officer, MuchGaming B.V.                            |
| Email Address      | compliance@crypto.games                                 |
| Registered Address | MuchGaming B.V., Curaçao                                |
| Platform           | <a href="https://crypto.games">https://crypto.games</a> |

9. Policy History

This is a new policy, prepared for submission to the Curaçao Gaming Authority in connection with the Company's gaming license (OGL/2024/1336/1047).

| Version | Effective Date | Approved By        | Description                                                                                                               |
|---------|----------------|--------------------|---------------------------------------------------------------------------------------------------------------------------|
| 1.0     | April 2026     | Board of Directors | Initial version, prepared for CGA submission pursuant to LOK (N.G. 2024, no. 157) and GCB AML Regulations (January 2025). |

10. Policy URL

This Policy is maintained as an internal compliance document of MuchGaming B.V. A summary AML/CFT statement is published on the Crypto.Games website at <https://crypto.games>, in the Legal / Compliance section of the platform. The full policy is available to the GCB and CGA upon request and is maintained by the AML Officer in the Company's compliance records.

APPROVAL AND SIGN-OFF

This Policy has been reviewed and approved by the Board of Directors of MuchGaming B.V.

| Board of Directors                                                                                                                                                                                                                                                                                                            | AML Officer      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <div>Signature: <div><div>Signed by:</div><div><div>8737E2B30CF043F...</div></div><div>Signed by:</div><div><div>E9C1A4A3F74E4ED...</div></div></div></div> | Signature: _____ |
| Name: Analissa Heiland & Lorenza Godett                                                                                                                                                                                                                                                                                       | Name: _____      |
| Date: 5/26/2026                                                                                                                                                                                                                                                                                                               | Date: _____      |