

# **Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing (AML, CTF, and CPF) Policy**

**Disrupt Entertainment Limited N.V.**

**Effective Date:** March 20<sup>th</sup>, 2026

**Version:** 2.1

# Table of Contents

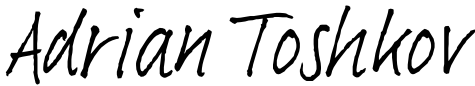
|                                                                                  |           |
|----------------------------------------------------------------------------------|-----------|
| <b>1. Introduction</b>                                                           | <b>5</b>  |
| 1.1    1.1    Policy Statement                                                   | 5         |
| 1.2    Purpose of this AML Policy                                                | 5         |
| 1.3    Definitions                                                               | 6         |
| <b>2. Regulatory Framework</b>                                                   | <b>8</b>  |
| <b>3. Scope</b>                                                                  | <b>8</b>  |
| <b>4. Governance and Responsibility</b>                                          | <b>8</b>  |
| 4.1    Managing Director                                                         | 8         |
| 4.2    Compliance Officer (MLRO)                                                 | 8         |
| <b>5. Risked Based Approach</b>                                                  | <b>9</b>  |
| 5.1    Business Risk Assessment (BRA)                                            | 9         |
| 5.1.1 Objectives of the Risk Assessment                                          | 9         |
| 5.1.2 Risk Categories Assessed                                                   | 9         |
| A.    Customer Risk                                                              | 9         |
| B.    Geographic Risk                                                            | 9         |
| C.    Product and Service Risk                                                   | 10        |
| D.    Transaction Risk                                                           | 10        |
| E.    Distribution Channel Risk Factors                                          | 10        |
| 5.1.3 Customer Risk Assessment (CRA)                                             | 10        |
| 5.1.4 Customer Acceptance Policy (CAP)                                           | 11        |
| 5.1.5 Application of Risk Assessment                                             | 11        |
| <b>6. Customer Due Diligence (CDD) and Know Your Customer (KYC)</b>              | <b>11</b> |
| 6.1    Purpose and Regulatory Alignment                                          | 11        |
| 6.2    Initial CDD                                                               | 12        |
| 6.3    Trigger Events for CDD                                                    | 12        |
| 6.4    Customer Identification Requirements                                      | 12        |
| A.    Identification and verification of customer                                | 12        |
| B.    Purpose and Nature of Business Relationship                                | 13        |
| C.    Ongoing Monitoring                                                         | 13        |
| D.    Behavior Monitoring                                                        | 13        |
| 6.5    Risk-Based Customer Classification                                        | 14        |
| 6.6    Simplified Due Diligence (Low Risk)                                       | 14        |
| 6.7    Enhanced Due Diligence (High Risk)                                        | 14        |
| 6.8    Ongoing Due Diligence and Monitoring                                      | 15        |
| 6.9    Sanctions, Politically Exposed Persons (PEPs) and Adverse Media Screening | 15        |

|                   |                                                         |           |
|-------------------|---------------------------------------------------------|-----------|
| 6.10              | Ongoing Monitoring and KYC Refresh                      | 16        |
| 6.11              | Termination of Business Relationship                    | 16        |
| <b>7.</b>         | <b>Crypto Asset Risk Management Framework</b>           | <b>17</b> |
| 7.1               | Risk-Based Approach to Crypto Assets                    | 17        |
| 7.2               | Wallet and Transaction Monitoring                       | 17        |
| 7.3               | Source of Funds (SoF) and Source of Wealth (SoW) Crypto | 18        |
| 7.4               | Travel Rule Compliance                                  | 18        |
| 7.5               | High-Risk Services and Anonymity Tools                  | 18        |
| 7.6               | Limits, Controls and Restrictions                       | 19        |
| 7.7               | Ongoing Monitoring and Red Flags                        | 19        |
| 7.8               | Record Keeping                                          | 19        |
| <b>8.</b>         | <b>Reporting Unusual Transactions</b>                   | <b>20</b> |
| 8.1               | Purpose                                                 | 20        |
| 8.2               | Unusual Transactions - Objective Indicators             | 20        |
| 8.3               | Unusual Transactions - Subjective Indicators            | 20        |
| 8.4               | Reporting Process                                       | 21        |
| 8.5               | Prohibition of Disclosure                               | 21        |
| 8.6               | Account Blocking                                        | 21        |
| <b>9.</b>         | <b>AML/CFT/CFP Compliance Program</b>                   | <b>22</b> |
| 9.1               | Compliance Officer                                      | 22        |
| 9.2               | Policies, Procedures and Controls                       | 22        |
| 9.3               | Employee screening                                      | 23        |
| 9.4               | Training Program                                        | 23        |
| 9.5               | Independent Audit                                       | 24        |
| <b>10.</b>        | <b>Branches and Subsidiaries</b>                        | <b>25</b> |
| <b>11.</b>        | <b>Governance</b>                                       | <b>25</b> |
| 12.1              | Board Approval                                          | 25        |
| 12.2              | Policy Updates                                          | 25        |
| 12.3              | Communication                                           | 25        |
| <b>12.</b>        | <b>Regulatory Examination</b>                           | <b>25</b> |
| <b>Appendix A</b> |                                                         | <b>26</b> |
| <b>Appendix B</b> |                                                         | <b>29</b> |
| <b>Appendix C</b> |                                                         | <b>31</b> |
| <b>Appendix D</b> |                                                         | <b>31</b> |

## Document Information

|                       |                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Subject</b>        | Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing (AML, CTF and CPF) Policy |
| <b>Impact</b>         | All Departments                                                                                                   |
| <b>Responsibility</b> | Money Laundering Reporting Officer                                                                                |
| <b>Approval</b>       | Board of Directors                                                                                                |
| <b>Review</b>         | Annually or As Needed                                                                                             |
| <b>Classification</b> | Company Confidential                                                                                              |
| <b>Effective date</b> | March 26 <sup>th</sup> , 2026                                                                                     |
| <b>Review date</b>    | April 26 <sup>th</sup> , 2027                                                                                     |

## Version History

|                                                                                                |                                                                                                                                                              |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Date</b>                                                                                    | March 26 <sup>th</sup> , 2026                                                                                                                                |
| <b>Version</b>                                                                                 | 2.1                                                                                                                                                          |
| <b>Summary Changes</b>                                                                         | Policy implementation                                                                                                                                        |
| <b>Approved by Management</b><br>Gouloud Hammoud<br>f/obo<br>Guardian Corporation Curaçao B.V. |                                                                          |
| <b>Approved by Compliance Officer</b><br>Adrian Toshkov                                        | <br><u>Adrian Toshkov</u><br>Adrian Toshkov (Apr 9, 2026 12:29:26 GMT+3) |

# 1. Introduction

## 1.1 Policy Statement

Disrupt Entertainment Limited N.V. (“the Company” or the “Company”) is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games on the internet, under the License No. OGL/2024/668/0844. In accordance with the license conditions, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorist Financing, and Counter Proliferation Financial (hereinafter “AML, CTF and CPF”) policy (hereinafter the “Policy”).

As a responsible gaming enterprise operating in Curaçao, the Company acknowledges the paramount importance of upholding the integrity of our financial systems and preventing the exploitation of our operations for unlawful activities. Our commitment to compliance transcends mere legal requirements; it is a core component of our corporate responsibility and ethical principles.

The company adopts a zero-tolerance approach to financial crime and ensures full transparency and cooperation with regulatory authorities.

## 1.2 Purpose of this AML Policy

The purpose of this Policy is to ensure the Company’s compliance with the relevant legal and regulatory requirements from the authorities in charge of the supervision of AML, CTF and CPF matters for the gaming sector are the Curaçao Gaming Authority (CGA) and the Financial Intelligence Unit Curaçao (FIU), while simultaneously ensuring the integrity and sustainability of the operations of the Company.

The following laws and regulations, as well as any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law, are applicable to the Company:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (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 Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Ordinance of the 20<sup>th</sup> of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Authority Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

As a member of the Financial Action Task Force ([www.fatf-gafi.org](http://www.fatf-gafi.org)) and of the Caribbean Financial Action Task Force ([www.cfatf-gafic.org](http://www.cfatf-gafic.org)), Curaçao is meeting international standards by regularly implementing the core standards of these organizations in its national legislation. These laws and standards oblige the Company to adopt risk-based procedures for customer due diligence, monitoring of transactions, and reporting of unusual activities.

By implementing this Policy, the Company aims to ensure that all employees understand and fulfill their legal and regulatory obligations. The Company will apply a risk-based approach to customer due diligence, transaction monitoring and the reporting of unusual activity. Additionally, this Policy seeks to foster a culture of compliance, transparency, and accountability across all levels of the organization.

From a business perspective, this Policy aims to protect the integrity of the Company's operations by preventing the platform from being exploited by criminal actors. It also seeks to safeguard the Company's reputation with customers, financial institutions, and regulatory authorities. Furthermore, maintaining eligibility for operating, licenses and business partnerships is a key objective, as the Company demonstrates compliance with relevant regulations. Finally, this Policy is designed to ensure business continuity by mitigating the legal, financial, and operational risks associated with AML/ CTF breaches.

### 1.3 Definitions

**Business Risk Assessment (BRA):** Assessment of ML/TF/FP risks the Company's business is generally exposed to.

**Customer Due Diligence (CDD):** Process of identifying customers and verifying their identity, understanding purpose of relationship, and ongoing monitoring.

**Customer Risk Assessment (CRA):** Customer-specific assessment categorizing ML/TF/FP risk as low, medium, or high.

**Enhanced Due Diligence (EDD):** Additional CDD measures for higher-risk situations.

**Financial Intelligence Unit (FIU):** Curaçao FIU receiving unusual transaction reports.

**Financial Transactions:** Deposits, withdrawals, and account funding (not gambling transactions).

**Politically Exposed Person (PEP):** Individual entrusted with prominent public function (foreign, domestic, or international organization). Many PEPs hold positions that can be abused for the purpose of laundering illicit funds or other predicate offences such as corruption or bribery. Because of the risks associated with PEPs, the FATF Recommendations require the application of additional AML/CFT measures to business relationships with PEPs. These requirements are preventive (not criminal) in nature and should not be interpreted as meaning that all PEPs are involved in criminal activity. PEP classification remains for a period after leaving office, typically around 12 to 18 months. Family members of a PEP include: a spouse or partner of the PEP; children of the PEP and their spouses or partners; and parents of a PEP are also considered PEP by association. Close associates of a PEP include: an individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP; and an individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.

**Domestic PEP:** Are individuals who are or have been entrusted domestically with prominent public functions, for example, heads of state or of government, senior politicians, members of parliament, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

**Foreign PEP:** Are individuals who are or have been entrusted with prominent public functions by a foreign country, for example, heads of state or heads of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

**International PEP:** An international politically exposed person refers to individuals who have been entrusted with a prominent function by an international organization. This includes members of senior management or individuals in equivalent roles, such as directors or board members. These individuals are considered politically exposed person (PEPs) due to their potential influence and the associated risks of corruption or bribery.

**Simplified Due Diligence (SDD):** Reduced CDD measures for lower-risk situations.

**Source of Funds:** How funds for particular transaction were obtained.

**Source of Wealth:** Origin of all money customers have accumulated over lifetime.

**Unusual Transaction:** Transaction meeting objective or subjective indicators per NORUT

## **2. Regulatory Framework**

This policy is aligned with:

- National Ordinance on Identification when Rendering Services (NOIS)
- National Ordinance on Reporting Unusual Transactions (NORUT)
- Sanctions National Ordinance
- Kingdom Sanction Act
- Curaçao Gaming Authorities regulations for combating ML/ TF/ FP (January 2025)
- Guidance and reporting obligations of the Financial Intelligence Unit Curaçao
- Applicable Curaçao AML/ CFT legislation

## **3. Scope**

This policy applies to:

- All employees, directors, and contractors
- All customers (B2C operators)
- All products and services, including crypto transactions
- All third-party providers (including crypto platforms)

## **4. Governance and Responsibility**

### **4.1 Managing Director**

The Managing Director holds ultimate responsibility for ensuring compliance with Curaçao Gaming Authority regulatory requirements and AML/ CFT obligations.

### **4.2 Compliance Officer (MLRO)**

The company appoints an independent Compliance Officer who:

- Oversees AML/ CFT compliance
- Acts as the primary contact with the Curaçao Gaming Authority
- Reports suspicious transactions to the Financial Intelligence Unit Curaçao
- Ensures implementation of internal controls
- Maintains AML documentation and audit readiness

## **5. Risk-Based Approach**

Disrupt Entertainment Limited N.V. implements a risk-based approach in accordance with Curaçao Gaming Authority expectations.

### **5.1 Business Risk Assessment (BRA)**

The Company conducts an annual Business Risk Assessment to identify, assess and mitigate ML/ TF/ FP risks considering:

#### **5.1.1 Objectives of the Risk Assessment**

The primary objectives are to:

- Identify inherent Aml-CFT risks within the business model
- Assess the effectiveness of existing controls
- Determine residual risk exposure
- Implement appropriate mitigation measures
- Ensure ongoing regulatory compliance

#### **5.1.2 Risk Categories Assessed**

The company evaluates risk across the following key categories:

##### **A. Customer Risk**

Includes factors such as:

- Customer identity and verification status
- Politically Exposed Person (PEP) status
- High-net-worth individuals
- Behavioral patterns and accounts with high activities
- Source of funds and wealth

##### **B. Geographic Risk**

Assessed based on:

- Customer country of residence
- Jurisdiction with weak AML/ CFT controls
- High-risk or sanctioned countries
- High-corruption countries
- Guidance from international AML bodies and regulatory authorities

## C. Product and Service Risk

Attention is given to:

- Cash transactions
- Peer-to-peer gaming
- Crypto-based transactions (high inherent risk)
- Instant deposits and withdrawals
- High-frequency gaming or trading activity
- Anonymity-enhancing features

## D. Transaction Risk

Includes:

- Transaction size and frequency
- Unusual or inconsistent activity
- Structuring (smurfing) patterns
- Rapid movement of funds
- Wallet-to wallet transfers

## E. Distribution Channel Risk Factors

Evaluates how customers interact with the platform:

- Non-face-to-face onboarding (online-only)
- Use of VPNs or anonymizing tools
- Use of third-party intermediaries
- Integration with external crypto platforms

### 5.1.3 Customer Risk Assessment (CRA)

For each customer, the Company performs a Customer Risk Assessment to categorize ML/ TF/ FP risk as:

| Risk Level | Description           |
|------------|-----------------------|
| Low        | Minimal risk exposure |
| Medium     | Moderate risk         |
| High       | Significant risk      |

The CRA determines the appropriate level of Customer Due Diligence (CDD) to be applied

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

The Company maintains a Customer Acceptance Policy that defines:

- Customer types presenting higher-than-average ML/ TF/ FP risk
- Risk indicators for low, medium, and high-risk classifications
- Level of CDD measures required for each risk category
- Circumstances warranting service refusal

Prohibited or restricted customer categories are:

- Sanctioned individuals or entities
- Anonymous or fictitious customers
- Customers from high-risk jurisdictions without Enhanced Due Diligence (EDD)

#### **5.1.5 Application of Risk Assessment**

The risk assessment directly influences:

- Customer onboarding requirements (KYC/ CDD/ EDD)
- Transaction monitoring
- Approval thresholds
- Frequency of reviews
- Reporting obligations

## **6. Customer Due Diligence (CDD) and Know Your Customer (KYC)**

### **6.1 Purpose and Regulatory Alignment**

Disrupt Entertainment Limited N.V. applies Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures to:

- Financial transactions equal or exceed XCG 4,000.00
- Carrying out occasional transactions above XCG 4,000.00
- Verify the identity of all customers
- Understand the nature and purpose of the business relationship
- Assess and mitigate AML/ CFT risks
- Ensure compliance with Curaçao regulatory requirements

This section is designed in accordance with the expectations of the Curaçao Gaming Authority and relevant AML/ CFT laws.

## **6.2 Initial CDD**

The company adheres to the following principles:

- No anonymous or fictitious accounts are permitted
- All customers must be identified and verified
- CDD must be completed before allowing unrestricted access to services
- A risk-based approach is always applied
- Customer information must be accurate, complete and up to date

## **6.3 Trigger Events for CDD**

CDD is performed in the following situations:

- Collect minimum identification at account opening at the onboarding stage (before full access is granted)
- Complete full CDD verification within 30 days of reaching XCG 4,000.00 threshold
- Before allowing withdrawals or high-value transactions
- When transaction deposit thresholds are reached: freeze further deposits/ withdrawals until CDD is complete
- When transaction withdrawals thresholds are reached: freeze account entirely until CDD is complete
- When there is suspicion of money laundering or terrorist financing
- When customer information changes or appears inconsistent
- When required by regulatory authorities
- Terminate relationship if CDD is not completed within 30 days

## **6.4 Customer Identification Requirements**

The company collects and verifies the following information at account opening:

### **A. Identification and verification of customer**

- Full legal name
- Permanent residential address
- Date of Birth

When the XCG 4,000.00 threshold is reached, additionally collect and verify:

- Place of Birth
- Nationality
- Identity number
- Residential address
- Contact details (email and phone number)

Customer identity must be verified using reliable and independent sources.

Accepted Documents:

- Government-issued documents
- Utility Bill (not older than 6 months)

### **B. Purpose and Nature of Business Relationship**

Understand the customers:

- Source of wealth (origin of accumulated money)
- Source of funds (how funds for specific transactions were obtained)
- Expected level of activity

Use statistical data or customer declarations appropriate to risk level

### **C. Ongoing Monitoring**

- Keep identification data accurate and up to date
- Monitor transactions for consistency with customer profile
- Investigate deviations from expected behavior
- Review customer risk assessment when patterns change

Monitoring is performed by a:

- Rule-based monitoring (thresholds, velocity checks, pattern detection)
- Automated vs manual monitoring processes
- Defined triggers for manual review and escalation
- Monitoring frequency based on risk classification

### **D. Behavior Monitoring**

The Company shall ensure that both financial transactions and gaming behavior form an integral part of transaction monitoring. In line with

regulatory expectations, monitoring shall not be limited to deposits and withdrawals but shall also include gambling related activity

- Analysis of betting patterns and behavioral trends
- Detection of chip dumping, collusion or coordinated activity between players
- Identification of bonus abuse, arbitrage and wash play

### **6.5 Risk-Based Customer Classification**

Each customer is assigned a risk level based on the company's risk assessment (see Section 5).

- Geographic location
- Transaction behavior
- Customer profile and occupation
- Use of crypto or anonymity tools
- PEP or sanctions exposure

### **6.6 Simplified Due Diligence (Low Risk)**

For low-risk customers:

- Limit identification to name, address, date of birth
- Reduce ongoing monitoring frequency
- Verify identity after establishing business relationships (if permitted by risk assessment)

### **6.7 Enhanced Due Diligence (High Risk)**

EDD is applied to high-risk customers, including:

- Politically Exposed Persons (PEP)
- Customers from high-risk jurisdictions
- Customers with high transaction volumes
- Suspicious or inconsistent activity

#### **Additional EDD measures for high-risk customers:**

- Obtain additional customer information (occupation, previous addresses)
- Obtain additional information on intended nature of relationship
- Verification of Source of Funds (SoF)

- Verification of Source of Wealth (SoW)
- Obtain senior management approval to establish or continue with the relationship
- Increase enhanced monitoring frequency
- Require first payment through reputable jurisdiction account

## **6.8 Ongoing Due Diligence and Monitoring**

CDD is not a one-time process. The company performs ongoing due diligence including:

- Continuous monitoring of transactions
- Periodic review of customer profiles
- Re-verification of identity where necessary
- Updates when risk levels change

Customer profiles are updated regularly to ensure accuracy and compliance completeness.

## **6.9 Sanctions, Politically Exposed Persons (PEPs) and Adverse Media Screening**

All customers and PEPs (foreign, domestic, international organization) are screened at the onboarding, before withdrawals and regularly during relationships against:

- UN Sanctions List
- EU Sanctions List
- OFAC Sanctions List
- Local Sanctions List (if published)
- Politically Exposed Persons (PEP) databases
- Adverse media sources

Any positive match is:

- Immediately escalated and account will be freeze
- Reviewed by the Compliance Officer
- Obtain senior management approval to establish or continue with the relationship
- Take reasonable measures to establish Source of Wealth and Source of Funds
- Reported to the Financial Intelligence Unit Curaçao where required
- Follow “Process for Freezing of Resources”

The same measures are applied to PEP family members and close associates.

If an existing customer becomes a PEP, the measures will be implemented within 30 days, or the relationship will be terminated.

#### **6.10 Ongoing Monitoring and KYC Refresh**

KYC is not a one-time process.

Continuous monitoring includes:

- Transaction behavior vs expected profile
- Changes in customer risk level
- Trigger events (large transactions, unusual patterns)

#### **KYC updates:**

|             |                             |
|-------------|-----------------------------|
| Low risk    | Every 2-3 years             |
| Medium risk | Every 1-2 years             |
| High risk   | Annually or more frequently |

#### **6.11 Termination of Business Relationship**

The relationship with the customer can be terminated if:

- Unable to complete CDD within required timeframe
- Customer refuses to provide required information
- Risk becomes unacceptable

The funds will be returned through the same channel they were received unless ML/ TF/ FP suspicion exists. The Financial Intelligence Unit will be reported if suspicion exists.

## **7. Crypto Asset Risk Management Framework**

### **7.1 Risk-Based approach to Crypto Assets**

The Company recognizes that the virtual assets present elevated risks due to their pseudonymous nature, cross-border functionality and potential misuse for money laundering and terrorist financing.

All crypto-related customers and transactions shall be subject to risk-based approach including:

- Classification of customers interacting with crypto as higher risk by default, unless proven otherwise
- Enhanced monitoring thresholds for crypto deposits, withdrawals, and gameplay-linked activity
- Segmentation of users based on wallet behavior, geography and transaction patterns

## **7.2 Wallet and Transaction Monitoring**

The Company shall implement blockchain analytics tools to monitor and assess crypto transactions in real-time or near real-time.

Controls shall include:

- Wallet risk scoring (e.g., exposure to darknet markets, sanctions, fraud or illicit services)
- Transaction tracing to identify origin and destination of funds
- Detection of high-risk typologies such as:
  - Rapid in-and-out transactions (layering)
  - Use of newly created wallets with no history
  - Multiple wallets hopping patterns
- Identification of links to high-risk jurisdictions or sanctioned entities

Any high-risk score shall trigger Enhanced Due Diligence (EDD) and potential account restrictions.

## **7.3 Source of Funds (SoF) and Source of Wealth (SoW) – Crypto**

For customers transacting in crypto, the Company shall apply enhanced verification measures.

This includes:

- Verification of the origin of crypto assets (e.g., exchange records, mining, trading activity)
- Requesting supporting documentation such as:
  - Screenshots or statements from exchanges or wallets
  - Transaction histories

- Assessment of consistency between declared wealth and crypto activity

Unverifiable or inconsistent SoF/ SoW shall result in:

- Transaction refusal
- Account suspension
- Filing of a Suspicious Activity Report (SAR)

#### **7.4 Travel Rule Compliance**

Where applicable, the Company shall comply with the Travel Rule requirements as recommended by the Financial Action Task Force (FATF).

This includes:

- Collection and transmission of required originator and beneficiary information for crypto transfers
- Cooperation with Virtual Asset Service Providers (VASPs)
- Ensuring proper record-keeping of transmitted data

#### **7.5 High-Risk Services and Anonymity Tools**

The Company strictly monitors and mitigates risks associated with privacy-enhancing technologies.

The following are considered high-risk indicators:

- Use of mixers/ tumblers (e.g., transaction obfuscation services)
- Privacy coins (where traceability is limited)
- Interaction with decentralized platforms lacking KYC controls

Where such risks are identified:

- Transactions may be blocked or rejected
- Accounts may be restricted pending investigation
- Enhanced monitoring and EDD shall be applied

#### **7.6 Limits, Control and Restrictions**

The Company shall implement specific controls for crypto transactions, including:

- Lower thresholds for anonymous or unverified wallets
- Mandatory KYC before withdrawal of crypto funds
- Limits on deposits and withdrawals based on risk level
- Prohibition of third-party wallet usage

### **7.7 Ongoing Monitoring and Red Flags**

The Company shall continuously monitor crypto activity and identify red flags such as:

- Discrepancy between gaming activity and transaction size (minimal play/ large withdrawals)
- Bonus abuse funded via cryptocurrency
- Repeated deposits followed by minimal gameplay
- Use of multiple accounts linked to similar wallet structures

Such cases shall trigger:

- Internal investigation
- Escalation to MLRO
- Potential SAR filing

### **7.8 Record Keeping**

All crypto-related transactions and associated data shall be securely recorded and retained in accordance with regulatory requirements.

This includes:

- Wallet addresses
- Transaction hashes
- Risk scores and monitoring results
- Customer communication and submitted documentation

## **8. Reporting Unusual Transactions**

### **8.1 Purpose**

The purpose of this section is to ensure that the Company:

- Timely identifies and reports unusual and suspicious transactions

- Complies with Curaçao Gaming Authority AML/ CFT reporting obligations
- Prevents the misuse of the platform for money laundering, terrorist financing, and fraud
- Maintains a clear audit trail for regulatory review

## **8.2 Unusual Transactions – Objective Indicators**

Report transactions  $\geq$  XCG 5,000.00 per gaming day:

- Cashless transactions (transfers from casino bank to customer bank)
- Deposits or withdrawal requests
- Sale of chips/tokens/credits to customer
- Cash outs
- Credit card and e-wallet transactions

## **8.3 Unusual Transactions - Subjective Indicators**

Report on transactions where:

- Reported to Police/Department of Justice for ML/TF connection
- Customer on sanctions list
- Presumption of ML/TF/FP exists based on:
  - Inconsistency with customer profile
  - Financial transactions are significantly greater than normal patterns
  - Gaming transactions inconsistent with normal pattern
  - Payment to blacklisted country bank account
  - Deposits/withdrawals to/from sanctioned person

## **8.4 Reporting Process**

The Company shall ensure that all suspicious activities are reported without delay and within clearly defined and measurable timeframes.

Procedures shall include:

### **1. Internal Reporting:**

- Immediate internal reporting of suspicious activity upon detection
- Clearly defined internal escalation timelines (e.g., within X hours)
- Review and decision making by the Money Laundering Reporting Officer (MLRO) within a specified timeframe

### **2. External Reporting:**

- The MLRO reports to the FIU within a maximum of 24 hours from the moment suspicion is confirmed

### **3. Documentation:**

- Maintain records of all reported and non-reported unusual transactions with rationale

## **8.5 Prohibition of Disclosure**

No employee may disclose to customers or third parties:

- That unusual transaction report has been filed
- That FIU has requested information
- Any details related to ML/TF/FP investigation

## **8.6 Account Blocking**

Internal procedures determine when unusual transaction reporting leads to account blocking, considering tipping-off risk.

## **RECORD KEEPING**

Maintain for minimum 5 years:

### **Customer Records:**

- Identification documents (copies of passports, ID cards, utility bills)
- CDD information and risk assessments
- Account files and business correspondence

- Evidence of beneficial ownership

**Transaction Records:**

- All customer transactions (domestic and international)
- Records sufficient to reconstruct individual transactions
- Source and recipient of payments

**Reporting Records:**

- Internal unusual transaction reports
- External reports to FIU
- Rationale for non-reporting decisions
- Records available to competent authorities upon appropriate legal request.

## **9. AML/CFT/CFP Compliance Program**

### **9.1 Compliance Officer**

**Appointment:** Senior officer at management level, independent from gaming operations

**Responsibilities:**

- Design and implement AML/CFT/CFP program
- Verify compliance with laws and regulations
- Review adherence to policies and procedures
- Organize staff training
- Analyze and review unusual transactions
- Report unusual transactions to FIU via goAML
- Maintain reporting records
- Update program as needed
- Monitor ML/TF/FP developments
- Prepare periodic reports for senior management/Board

**Current Compliance Officer:** Adrian Toshkov

### **9.2 Policies, Procedures and Controls**

The Company maintains written, Board-approved:

- AML/CFT/CFP policies
- Customer Acceptance Policy
- CDD procedures
- Transaction monitoring procedures
- Reporting procedures
- Record-keeping procedures
- Risk management measures
- Sanctions screening procedures

Policies are reviewed annually and updated as needed.

### 9.3 Employee screening

All employees undergo criminal background checks before hiring.

### 9.4 Training Program

New Employees:

- Nature and process of ML/TF/FP
- Internal policies and procedures
- ML methods and trends in gambling sector
- CDD requirements
- Objective and subjective reporting indicators

Role-Specific Training:

- **Dealers/Cashiers:** Front-line ML detection, transaction monitoring
- **Supervisors/Managers:** Comprehensive ML/TF/FP oversight
- **Compliance Staff:** Specialized AML/CFT/CFP training
- **Senior Management/Board:** Reputational risk awareness

Ongoing Training:

- Refresher training at regular intervals (annual)
- The training will be in the form of testing, and a certification will be granted at the end
- There will be a minimum test pass criteria and recordkeeping of results
- Updates on new ML/TF/FP trends and techniques
- Regulatory changes

#### Training Records Maintained:

- Training content
- Attendee names and dates
- Test results
- Ongoing training plan

### **9.5 Independent Audit**

An independent audit function will be established for the annual evaluation of the AML program, ensuring audit personnel are qualified and findings are documented. The audit must include several key assessments, such as:

- Reviewing the Company's AML, CTF and CPF manual.
- Examining customer files.
- Evaluating compliance management.
- Conducting transaction testing.
- Assessing the adequacy of training.
- Ensuring compliance with relevant laws and regulations.
- Evaluating the system's capacity to detect unusual activities.
- Interviewing employees involved in transactions and their supervisors
- Sampling unusual transactions and reviewing compliance with internal and external policies and reporting requirements.
- Assessing the effectiveness of the record retention system.

The audit shall also evaluate the Company's responsiveness to previous audit findings. All testing scopes and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

## **10. Branches and Subsidiaries**

Foreign branches and subsidiaries must implement AML/CFT/CFP measures consistent with Curaçao requirements.

## **11. Governance**

### **11.1 Board Approval**

This policy is approved by the Board of Directors and reviewed annually.

### **11.2 Policy Updates**

Policy updated when:

- Regulatory changes occur
- BRA identifies new risks
- Audit identifies deficiencies
- New products/services/delivery channels introduced

### **11.3 Communication**

Policy communicated to all employees through:

- Training sessions
- Internal announcements
- Accessible policy repository

## **12. Regulatory Examination**

The Company provides to Curaçao Gaming Authority upon request:

- Written AML Compliance Program
- Business Risk Assessment records
- Compliance Officer identification and job description
- Unusual transaction reports (internal and external)
- Frozen account records
- Training records
- Independent audit reports
- Customer files (risk assessments, CDD, acceptance, transaction information)

## **APPENDIX A:**

### **Country Risk List:**

Please note that the following list of high-risk and low-risk countries is subject to continuous review. Any changes in geographical risk will be reflected promptly to ensure the list remains current and accurate at the time of drafting.

#### High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Belarus
5. Bulgaria
6. Burkina Faso
7. Burma (Myanmar)
8. Cameroon
9. Central African Republic
10. China
11. Côte d'Ivoire
12. Croatia
13. Cuba
14. Democratic People's Republic of Korea.
15. Democratic Republic of the Congo
16. Ethiopia
17. Gibraltar
18. Haiti
19. Iran
20. Iraq
21. Kenya
22. Lebanon
23. Libya
24. Mali
25. Monaco
26. Mozambique
27. Namibia
28. Nicaragua
29. Nigeria
30. Panama

31. Philippines
32. Russia
33. Somalia
34. South Africa
35. South Sudan
36. Syria
37. Tanzania
38. Uganda
39. United Arab Emirates
40. Vanuatu
41. Venezuela
42. Vietnam
43. Yemen

Low-risk countries include:

1. Antigua and Barbuda
2. Aruba, Kingdom of the Netherlands
3. Belize
4. Bermuda
5. Cayman Islands
6. Denmark
7. Dominica
8. Finland
9. Grenada
10. Guyana
11. Montserrat
12. New Zealand
13. Norway
14. Saint Kitts and Nevis
15. Saint Lucia
16. Saint Vincent & the Grenadines
17. Singapore
18. Sint Maarten Kingdom of the Netherlands
19. Suriname
20. Sweden
21. Turks and Caicos Islands

Excluded markets include, but are not limited to:

1. Aruba

2. Australia
3. Austria
4. Belgium
5. Bonaire
6. Czech Republic
7. Curacao
8. France
9. Germany
10. Greece
11. Lithuania
12. Saba
13. Sint Eustatius
14. Spain
15. The Netherlands
16. United States of America

## APPENDIX B

| Internal Unusual Activity Report                                                                                                                            |            |       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-------|
| Date of report:                                                                                                                                             |            |       |
| Client full name:                                                                                                                                           |            |       |
| Client ID:                                                                                                                                                  |            |       |
| Risk rating:                                                                                                                                                |            |       |
| Account status<br>(Active/Suspended/Blocked):                                                                                                               |            |       |
| Account balance:                                                                                                                                            |            |       |
| Date of account registration:                                                                                                                               |            |       |
| Client details: E-mail:                                                                                                                                     |            |       |
| Client details: Phone number:                                                                                                                               |            |       |
| Client details: Brand<br>registration:                                                                                                                      |            |       |
| Date of birth:                                                                                                                                              |            |       |
| Nationality/Country of<br>registration:                                                                                                                     |            |       |
| Address:                                                                                                                                                    |            |       |
| Due diligence documents held:                                                                                                                               |            |       |
| Reason for reporting: explain<br>what activity / transaction gave<br>rise to the report.<br>If necessary, please use the<br>additional information section: |            |       |
| Date of suspected criminal<br>activity/transaction:                                                                                                         |            |       |
| Provide details (e.g. dates and<br>amounts) of any known intended<br>or pending transactions:                                                               |            |       |
| Name (reporting employee):                                                                                                                                  | Signature: | Date: |
|                                                                                                                                                             |            |       |

|                                                                                                                      |            |       |
|----------------------------------------------------------------------------------------------------------------------|------------|-------|
| Upon completion, please forward the form to the department responsible as soon as possible.                          |            |       |
| Action taken by the responsible department                                                                           |            |       |
| Confirmation of receipt of the MLRO:<br><br>I confirm that I have received this form from the person(s) named above. | Signature: | Date: |

## APPENDIX C:

### SANCTIONS LISTS RESOURCES

- **UN Sanctions:** <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>
- **EU Sanctions:** <http://www.sanctionsmap.eu/#/main>
- **FATF Lists:** [www.fatf-gafi.org](http://www.fatf-gafi.org)
- **CFATF Statements:** [www.cfatf-gafic.org](http://www.cfatf-gafic.org)
- **Transparency International Corruption Index:** [www.transparency.org](http://www.transparency.org)

## APPENDIX D:

### INDICATORS CHECKLIST

#### Objective Indicators (≥XCG. 5,000.00 per gaming day):

- ☐ Cashless transaction
- ☐ Deposit or withdrawal request
- ☐ Chip/token/credit sale
- ☐ Cash out
- ☐ Credit card transaction
- ☐ E-wallet transaction

#### Subjective Indicators:

- ☐ Reported to Police/Justice for ML/TF
- ☐ Customer on sanctions list
- ☐ Transaction inconsistent with customer profile
- ☐ Significantly greater transaction value than normal
- ☐ Gaming pattern inconsistent with normal
- ☐ Payment to blacklisted country
- ☐ Transaction with sanctioned person