

ZOZO TECHNOLOGY B.V.

ANTI-MONEY LAUNDERING POLICY

Approval	Board of Directors
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	April 10, 2025
Version	1.1 — 24 March 2026 (supersedes v1.0)
Next Review Date	May 30, 2027

Policy History

Date	Ver.	Summary of Changes	
6 October 2025	1.0	Initial policy implementation	
24 March 2026	1.1	Following CGA Notice ADMIN-20565, the following changes were made from v1.0: 1. §5.1 — Four-stage onboarding model introduced: Stage 1 (account creation — email, username, password only); Stage 2 (email OTP verification + full KYC form + ID upload combined, triggered before first deposit); Stage 3 (jurisdiction check); Stage 4 (deposit activation). 2. §5.1 — Mandatory KYC fields at registration updated to NOIS/CGA minimum requirements only: full name, date of birth, place of birth, residential address, nationality, ID number, and government-issued ID document upload. Occupation fields collected during CDD/EDD process where applicable. 3. §4.2 — Restricted Jurisdictions framework added with definitive Restricted Jurisdictions List (Appendix I) enforced via onboarding drop-down and IP geo-blocking. 4. Appendix I — New: Restricted Jurisdictions List (27 entries, 7 regional groups).	Compliance Officer, Zozo Technology B.V.


Emmanuel Waruga Kimani
Compliance Officer


Gouloud Hamoud
f/obo Guardian Corporation Curaçao B.V.
Statutory Director

TABLE OF CONTENTS

- 1. Introduction
 - 1.1 Policy Statement
 - 1.2 Purpose of this AML Policy
 - 1.3 Definitions
- 2. Policy Implementation
- 3. The Risk-Based Approach
- 4. Customer Acceptance Policy
 - 4.1 Customer Risk Assessment
 - 4.2 Prohibited Accounts & Restricted Jurisdictions ← UPDATED v1.1
 - 4.3 Politically Exposed Persons (PEPs)
 - 4.4 Sanctions Screening
- 5. Customer Due Diligence (CDD) Measures
 - 5.1 Customer Onboarding and Identification ← UPDATED v1.1
 - 5.2 Verification of Beneficial Ownership
 - 5.3 Customer Risk Assessment and Purpose of Relationship
 - 5.4 Simplified Due Diligence (SDD)
 - 5.5 Customer Due Diligence (CDD)
 - 5.6 Timeline for Compliance and Non-Compliant Documents
 - 5.7 Enhanced Due Diligence (EDD)
 - 5.8 Ongoing Monitoring
 - 5.9 Reliance on Third Parties
- 6. Reporting of Unusual Transactions
- 7. Anti-Money Laundering Compliance Program
- 8. Compliance and Consequences of Non-Compliance
- Appendix I — Restricted Jurisdictions List ← NEW v1.1

1. INTRODUCTION

1.1. POLICY STATEMENT

Zozo Technology B.V. (the "Company") is licensed and regulated by the Curaçao Gaming Authority (CGA) to offer remote (online) games on the internet, under License No. OGL/2024/1519/0809. The Company has developed this comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing ("AML, CTF and CPF") policy in accordance with its license conditions.

As a responsible gaming enterprise, the Company acknowledges the paramount importance of upholding the integrity of its financial systems and preventing the exploitation of its operations for unlawful activities.

1.2. PURPOSE OF THIS AML POLICY

This Policy ensures the Company's compliance with applicable AML, CTF and CPF legal and regulatory requirements supervised by the CGA and the Curaçao Financial Intelligence Unit (FIU). Applicable legislation includes:

- 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 on penalties and fines for reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6
- Ministerial Decree — 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 (PB 2024, no. 157)
- CGA Regulations for combating Money Laundering, Terrorism Financing and Proliferation Financing, last update January 2025

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (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

CFATF means The Caribbean Financial Action Taskforce, an organization of twenty-four (24) states of the Caribbean Basin, Central and South America, which have agreed to implement common countermeasures to address money laundering.

Compliance Officer means A senior officer at management level and independent from the games' operations, responsible for the detection and deterrence of money laundering and terrorist financing.

FATF means The Financial Action Task Force. An independent intergovernmental body, established in 1989 and mandated by its Member Jurisdictions to develop and promote policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

FATF Recommendations means A framework of recommendations on policies and measures, issued by the FATF, to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction;

Financial Transactions include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens. Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

Financing of proliferation (PF) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

FIU means The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT.

Kingdom Sanctions Act means The National Ordinance also known as the "Rijkssanctiewet", published under N.G. 2016 no. 54.

Money laundering (ML) is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the

"placement" stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

NOIS means National Ordinance on Identification of Clients when rendering Services (Landsverordening identificatie bij dienstverlening, N.G. 2017, no. 92).

NORUT means National Ordinance on the Reporting of Unusual Transactions (Landsverordening Melding Ongebruikelijke Transacties, N.G. 2017, no. 99).

Politically Exposed Persons (PEPs) means: Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are: Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials, and the direct family members or close associates of such persons. Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions, and the direct family members or close associates of such persons.

Sanctions National Ordinance means The National Ordinance also known as the "Sanctielandsverordening", published under N.G. 2014 no. 55.

Source of Funds Refers to how the funds for a particular transaction were obtained by the player, like personal savings, pension release, property sales, share sales and dividends, gambling winnings, gifts, compensation from legal rulings.

Source of Wealth is the origin of all the money a person has accumulated over their lifetime, like employment income, inheritances, investments, business ownership interests.

Targeted financial sanctions are measures imposed by governments or international bodies to restrict the financial activities of specific individuals or entities linked to unlawful activities, such as terrorism or money laundering. These sanctions aim to prevent these parties from accessing the financial system. Unlike general sanctions that apply broadly

to entire countries, targeted sanctions focus on specific individuals or entities. This approach minimizes the impact on the wider population while addressing particular risks. Targeted financial sanctions apply to individuals or entities listed on sanctions lists maintained by organizations like the United Nations or the European Union.

Terrorism Financing (TF) refers to the provision of funds or financial support for terrorist acts, individuals, or organizations, and is characterized by the intent to intimidate populations or compel governments and international bodies to act or refrain from acting. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.

Unusual transaction A transaction that is considered as such on the basis of certain indicators, pursuant to Article 10 of the N0RUT.

(Ultimate) beneficial ownership (UBO) Refers to the natural person(s) who ultimately own(s) or control(s) a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person.

2. POLICY IMPLEMENTATION

The Company internal controls are a set of policies and procedures aimed at securing the efficient and compliant business within the Company and provision of the safe and fair gambling environment for the customers. Internal controls in relation to ML&TF risks consist primarily of systematic application of the rules and procedures laid out in the corresponding sections of this Policy and the Regulations.

2.1. RESPONSIBILITY OF THE SENIOR MANAGEMENT

The Senior Management is responsible for:

- setting and approving the general principles underlying the Policy for Prevention and Combatting of Money Laundering and Terrorist Financing
- appointing Compliance Officer and communicating to them the internal policies
- defining the duties and responsibilities of the Compliance Officer

- ensuring that effective and sufficient systems and controls are in place to enable compliance with all rules and regulations
- ensuring that the Compliance Officer have completed and timely access to all data required to effectively undertake their duties including, but not restricted to, data concerning customer identity, transaction documentation and other relevant information maintained
- ensuring that all employees are aware to whom they have to report any information concerning unusual transactions
- ensuring that the Compliance Officer have sufficient resources including competent staff and technological equipment
- assessing and approving the annual report and taking appropriate actions to remedy any weaknesses and/or deficiencies identified in the annual report.

2.2. AML & TF Compliance Officer

The Compliance Officer has working knowledge of the Company's business environment, risks inherent to the Company's business model and AML&TF provisions as stipulated in the Regulations as amended. AML&TF Compliance Officer also performs the duties of Money Laundering Reporting Officer and is responsible for reporting transactions unusual from AML&TF standpoint to Senior management in accordance with Section RESPONSIBILITY OF **THE** Senior Management hereof.

General duties of the AML&TF Compliance Officer include monitoring of the Company's compliance with the AML&TF obligations, assessment of the business risks both internal and external, oversight of the AML&TF related communication and training for employees and reporting of the findings and critical issues of the AML&TF systems and procedures to the managers and executives of the Company.

2.3. EMPLOYEES

2.3.1 STAFF RELIABILITY AND PROBITY

The Company has established HR policies and procedures for effective initial candidate screening and ongoing employee management. All personnel undergo a personal identification process, and candidates must complete an ID profile that includes psychological tests during their first interview to assess potential risks. After the initial interview, successful candidates participate in a second interview with the HR Director, followed by discussions with the subject area manager and a member of the internal security department. A thorough background check is conducted, which includes contacting previous supervisors, verifying criminal records, and reviewing job references.

Once candidates successfully complete the screening process, they are required to undergo a mandatory three-week introductory training course divided into five stages, covering bookmaking basics, payment systems, software usage, customer complaint handling, and workplace training. After passing all exams, new employees begin their roles under close

supervision. For executive positions, candidates must have a personal interview with the CEO or owner before a hiring decision is made.

2.3.2 STAFF RELIABILITY AND PROBITY

The Company is committed to supporting employees' professional development through various training opportunities, including on-site and remote training, technical seminars, and workshops. Employees receive training in relevant business areas, with management training focusing on effective management practices and business English courses available for all staff. Specialized professional upgrade courses are conducted internally for Trading and Operational Department staff, while the Marketing and Finance Departments participate in targeted training sessions relevant to their fields.

In addition, refresh training sessions are conducted periodically, at least annually, to ensure employees remain up-to-date with current practices. Specific events, such as the introduction of new systems or technologies-especially those that have a higher potential for misuse in money laundering-will trigger additional training sessions. Significant violations of this policy will also prompt targeted training to reinforce compliance expectations.

Additionally, the Compliance Officer conducts mandatory introductory Anti-Money Laundering and Terrorism Financing (AML&TF) training for all new employees, which covers their roles in compliance, identifying red flags for money laundering, and the procedures for reporting suspicious activities. This training is supplemented with updates on the latest tools and practices in AML&TF investigations. The Compliance Officer maintains a register of all trained employees involved in monitoring transactions and compliance management.

3. THE RISK-BASED APPROACH

3.1. EXPLANATION OF THE RISK-BASED APPROACH

The Company adopts a risk-based approach in our AML compliance program, as recommended by FATF guidelines. This approach is essential for identifying and mitigating ML/TF/PF risks specific to the online gaming industry. When developing its AML compliance program, the Company assesses risks in such a way that higher risks necessitate more robust measures to mitigate them. Conversely, for lower-risk scenarios, the Company may employ simplified measures.

To effectively apply the risk-based approach, the Company conducts a preliminary assessment of the risks associated with money laundering and terrorist financing within the organization, and based thereon develops and implements suitable policies, procedures, and controls to manage and mitigate these identified risks, including the present Policy.

The Company shall continuously monitor and enhance the effectiveness of these policies, procedures, and controls, ensuring that it maintains thorough documentation of its risk assessments, detailing all actions taken and the rationale behind them. The Company shall also assess and manage risks associated with emerging technologies and new gaming products that may facilitate ML/TF/PF activities.

3.2. BUSINESS RISK ASSESSMENT

The Business Risk Assessment (BRA) framework is a crucial component of The Company's AML, CTF, and CPF compliance program. It provides a systematic, risk-based approach for identifying, assessing, and mitigating money laundering, terrorist financing, and proliferation financing risks within the Company's operations.

The Company performs thorough BRAs, evaluating potential risk factors related to customers, products and services, geographic locations, and delivery channels. Each risk factor is assessed for its likelihood and potential impact. Tailored controls and measures are then implemented to address these risks. All findings, evaluations, and mitigation strategies are documented and reported to senior management and relevant regulatory authorities.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed regularly. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment.

4. CUSTOMER ACCEPTANCE POLICY

4.1. CUSTOMER RISK ASSESSMENT

The Customer Risk Assessment procedure is a crucial component of the internal AML program at the Company, designed to evaluate the specific risks associated with providing services or products to customers. The assessment begins when a new customer applies for an account, at which point their risk profile is formulated based on the information collected. The initial Customer Risk Rating assigned helps determine the frequency and intensity of ongoing reviews; higher-risk customers will be subject to more frequent and rigorous monitoring.

The assessment process considers several key factors:

- **Customer Risk:** This involves evaluating the customer's background, occupation, and transaction patterns. Higher-risk categories include customers with multiple or irregular income sources, politically exposed persons (PEPs), high spenders, disproportionate spenders (whose spending habits do not align with their known income), and those using third parties to gamble in ways that may circumvent customer due diligence measures.

- **Product/Service Risk:** This factor assesses the risks associated with the casino's offerings. Certain gaming products or services, especially those allowing customers to influence outcomes, pose higher risks. Payment methods are also evaluated, with specific high-risk factors including anonymous payment options (like pre-paid cards and virtual assets), unusual account usage, peer-to-peer gaming, and multiple accounts or wallets. Additionally, identity fraud and the use of unlicensed electronic wallets are considered significant risks.
- **Geographic Risk:** The geographic location of the customer and the transaction is assessed, with higher risk assigned to customers from countries with weak AML regulations or high corruption levels. Relevant sources of information include the FATF lists of high-risk jurisdictions, the U.S. Department of State's International Narcotics Control Strategy Report, and other credible indices. The nationality, residence, and place of birth of the player are also taken into account.
- **Delivery Channel Risk:** This involves evaluating the methods used to establish a business relationship or conduct transactions. Channels that favor anonymity and non-face-to-face interactions are considered higher risk, prompting the Company to implement reasonable measures to mitigate these risks.

After the assessment, customers are categorized as low, medium, or high risk. The level of due diligence and ongoing monitoring applied corresponds to their risk classification:

- For customers assessed as low risk, a Simplified Due Diligence process will be applied, provided they do not exhibit any risk-enhancing characteristics and their transactions remain below the threshold of Cg. 4,000.
- Medium and high-risk customers will require additional information and documentation in accordance with the Company's policies.
- Accounts classified as high risk or displaying potentially suspicious behavior will be reviewed by compliance personnel and reported to the Compliance Officer (CO) for further investigation.

This structured approach ensures that the company effectively identifies and mitigates the risks associated with its customers, aligning with regulatory expectations and promoting a robust AML compliance program.

4.2. PROHIBITED ACCOUNTS & RESTRICTED JURISDICTIONS [UPDATED — v1.1]

4.2.1 PROHIBITED ACCOUNTS

The following categories of individuals are prohibited from being accepted as customers:

- Individuals under the age of 18
- Individuals listed on sanctions imposed by the UN, EU, or OFAC
- Individuals for whom there are reasonable grounds to suspect involvement in ML/TF/PF or any other form of criminal activity

- Self-excluded customers barred from our websites or included in any national self-exclusion register as stipulated by licensing conditions
- Individuals who have submitted documents or information reasonably suspected to be fraudulent or falsified

4.2.2 RESTRICTED JURISDICTIONS [NEW — v2.0]

The Company maintains a Restricted Jurisdictions List (set out in full in Appendix I) comprising all countries and territories from which the Company does not hold the necessary regulatory authorization, or where online gaming is otherwise prohibited under applicable local law.

The Restricted Jurisdictions List is enforced through two complementary technical controls:

- **Primary control — Onboarding drop-down gate:** At Stage 2 of the onboarding process (see §5.1), customers must select their country of residence. Countries appearing on the Restricted Jurisdictions List are excluded from the selectable options or, where technically necessary, trigger a 'service not available' notification that prevents the customer from proceeding.
- **Secondary control — IP-based geo-blocking:** The Company operates IP-level geo-blocking as a secondary layer to prevent access from restricted jurisdictions, including for customers who may attempt to circumvent the onboarding drop-down control.

The Restricted Jurisdictions List shall be:

- Reviewed and formally approved by the Compliance Officer at least annually, or following any material change in the Company's licensing position, applicable CGA guidance, or relevant FATF designations
- Cross-referenced against the FATF list of high-risk and other monitored jurisdictions, the U.S. Department of State's International Narcotics Control Strategy Report (INCSR), and the Company's CGA license conditions
- Maintained as Appendix I to this Policy, updated at each annual review, and made available to CGA examiners upon request in accordance with §7.4

4.3. POLITICALLY EXPOSED PERSONS (PEPs)

The Company implements robust procedures for identifying and managing relationships with PEPs, defined as individuals entrusted with prominent public functions, as well as their close associates and family members.

- **Identification:** Comprehensive screening against reliable databases will be conducted during the onboarding process to determine PEP status.
- **Approval Process:** No business relationship shall be established or continued with a PEP without obtaining senior management approval.
- **Source of Wealth and Funds:** The Company will request a statement from the PEP regarding their source of wealth and verify this information through independent and reliable sources. Additional documentation may be requested if necessary.
- **Enhanced Monitoring:** The Company will conduct enhanced ongoing monitoring of

PEPs, analyzing their spending patterns to ensure they align with declared legal sources of funds.

PEP status screening will occur regularly throughout the business relationship. If a customer not identified as a PEP at onboarding later becomes one, the Company will implement enhanced due diligence measures within 30 days. Failure to implement these measures will result in the termination of the relationship with that customer.

4.4. SANCTIONS SCREENING

The Company is committed to complying with targeted financial sanctions, which require the freezing of funds and assets of individuals and entities identified by the UN and EU as involved in terrorism or proliferation activities.

- **Ongoing Monitoring:** The Company will perform ongoing sanctions screening at key points, including during registration, withdrawal requests, and any changes to personal details or payment methods.
- **Action on True Matches:** If a true match is discovered, the Company will immediately freeze the funds of the affected customer and file a report with the Financial Intelligence Unit (FIU). Services will be terminated upon confirmation of the true match by the supervisory authority, and frozen assets will be held until further instructions are received.

5. CUSTOMER DUE DILIGENCE (CDD) MEASURES

5.1. CUSTOMER ONBOARDING AND IDENTIFICATION [UPDATED — v1.1]

The Company operates a staged onboarding model designed to ensure full AML/KYC compliance under NOIS and CGA licensing conditions, while providing a clear and structured customer journey. No financial activity — including deposits, withdrawals, or wagering with real funds — is permitted until all applicable onboarding stages have been successfully completed.

5.1.1 THE FOUR STAGE ONBOARDING GATE

Stage	Gate	Requirements
1	Account creation	Email address, username, and password only. Account is created but all financial activity is disabled. No KYC data is collected at this stage. This mirrors industry standard practice.

2	Email OTP verification & KYC data collection	When the customer initiates their first deposit, they are prompted to verify their email address via a one-time passcode (OTP) and complete the full KYC form in the same step. The following must be provided before deposit functionality is enabled: • Full legal name (first and last) • Country of residence • Place of birth • Date of birth • Permanent residential address (street, city, postal code) • Nationality • Identification number • Upload of a valid government-issued ID document (passport, national ID card, or driver's license — must include photograph and be legible) Deposit functionality remains locked until all of the above are successfully submitted.
3	Jurisdiction check	The system validates the customer's country of residence against the Restricted Jurisdictions List (Appendix I). Customers from restricted jurisdictions receive a 'service not available' notification and cannot proceed.
4	Deposit & financial activity enabled	Only after successful completion of Stages 1–3 is the customer's wallet and deposit functionality activated. No financial transactions are permitted prior to completion of all preceding stages.

5.1.2 MANDATORY KYC DATA FIELDS (Stage 2)

The following fields are the minimum mandatory requirements under NOIS and CGA licensing conditions and must be submitted — together with email OTP verification — before deposit functionality is enabled:

- Full legal name (first name and last name)
- Country of residence — validated against the Restricted Jurisdictions List (Appendix I)
- Place of birth
- Date of birth
- Permanent residential address (street address, city, and postal code)
- Nationality
- Identification number
- Upload of a valid government-issued identification document (passport, national ID card, or driver's license) — must include a photograph and be legible

Where an identity document is not in a language understood by the Company, a certified translation may be required. Proof of permanent residential address dated within the last 6 months (e.g., utility bill or bank statement) must also be provided. The Company prohibits anonymous and fictitious accounts and applies robust technical controls to prevent their creation.

5.1.3 NON-COMPLIANT DOCUMENTS

Where a document submitted at Stage 3 does not meet verification standards, the designated compliance staff member must immediately flag it, inform the customer of the specific reason for non-compliance, and provide a reasonable opportunity to resubmit. All actions, communications, escalations, and outcomes must be recorded in the customer's file to ensure a complete audit trail.

5.2. VERIFICATION OF BENEFICIAL OWNERSHIP

Customers must confirm they act on their own behalf. The Company monitors for

indications of third-party control. The following safeguards apply:

- Payment method verification: deposits and withdrawals must be made using accounts in the customer's name.
- Monitoring for proxy activity or suspicious behavior.
- Immediate verification upon withdrawal requests or Cg. 4,000 thresholds.

5.3. CUSTOMER RISK ASSESSMENT AND PURPOSE OF RELATIONSHIP

Each customer is assigned a risk rating based on:

- Jurisdiction of residence;
- PEP or sanctions status;
- Payment method used;
- Anticipated transaction volumes and types.

The customer must provide their occupation and estimated annual income. This information is verified proportionally to the assessed risk. For High-Risk customers, supporting documentation (e.g., pay slips, bank statements, tax returns) is required.

Occupation information is collected as part of the CDD/EDD process when required by the customer's risk profile or upon reaching the Cg. 4,000 thresholds, in line with the risk-based approach.

5.4. SIMPLIFIED DUE DILIGENCE (SDD)

SDD may be applied only where:

- The customer is classified as low risk;
- No suspicion of ML/TF exists;
- No indicators of PEP status or high-risk jurisdiction are present;
- The total transaction value is below Cg. 4,000.

Under SOD:

- Basic identification is collected;
- Verification may be delayed until specific thresholds are met;
- Monitoring is tailored based on risk, and must still detect unusual activity.

If risk increases or suspicious behavior arises, SOD must be upgraded to COD or EDD.

5.5. CUSTOMER DUE DILIGENCE (CDD)

CDD must be performed:

- When the customer reaches the Cg. 4,000 threshold (cumulatively or per transaction);
- On all withdrawals;
- When doubts arise about prior CDD data;
- When required under NORUT or due to suspicion of ML/TF/PF.

All financial transactions (excluding bonuses or winnings) are counted toward the threshold. Identification and verification must be complete before allowing further transactions.

5.6. TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS

If the customer cannot provide compliant documents within 30 days from the moment the Cg. 4,000 threshold is reached, the Company shall terminate the relationship with the customer and consider filing an Unusual Activity Report with the FIU, provided that a presumption of ML or TF exists.

During the COD process, customers may continue to access their accounts while the Company gathers the necessary information. However, if a deposit reaches the Cg. 4,000 thresholds, the customer will be prohibited from further deposits or withdrawals, although they may continue to play with their existing balance. Conversely, if the threshold is reached due to a withdrawal request, the account will be completely frozen, halting all gameplay.

If a document submitted by a (potential) customer does not meet the verification standards, the designated staff member must immediately flag it for further examination. The initial review should be thorough to pinpoint the specific reasons for non-compliance. Once a non-compliant document is identified, the customer must be informed without delay.

All actions taken in response to non-compliant documents shall be carefully recorded. This includes the initial identification of the issue, communications with the customer, any escalations, and the final outcome. Comprehensive records should be maintained in the customer's file to ensure a complete audit trail.

5.7. ENHANCED DUE DILIGENCE (EDD)

The Company shall implement Enhanced Due Diligence (EDD) measures for customers identified as higher risk, with actions tailored to the specific risks identified during the assessment process. These measures aim to intensify monitoring of the business relationship to detect any unusual or suspicious transactions or activities. EDD is required in situations where the risk of ML, TF or PF is heightened.

In any case, the following scenarios are subject to EDD:

- *Residents of High-Risk Geographic Areas:* Customers residing in jurisdictions associated with higher levels of corruption or inadequate AML, CTF, and CPF regulations.
- *Politically Exposed Persons (PEPs):* Individuals who hold prominent public positions or are closely connected to such individuals, which may elevate the risk of corruption.
- *Anonymity-Favoring Products or Transactions:* Services or products that allow for a higher degree of anonymity, potentially facilitating illicit activities.

- *New Products and Business Practices:* The introduction of new services, technologies, or delivery mechanisms that may present unforeseen risks.

The measures applied during EDD must align with the identified risks and may include, but are not limited to:

- *Additional Customer Information:* Collect comprehensive information about the customer, including occupation, previous addresses, and relevant data from public databases and online resources.
- *Clarification of Business Relationship Intent:* Obtain further information regarding the intended nature of the business relationship to better understand the customer's gaming habits and expectations.
- *Source of Funds and Wealth (SOF/SOW):* Gather detailed information on the source of funds or wealth for the player. Examples include:
 - Personal savings
 - Employment income
 - Pension releases
 - Share sales and dividends
 - Property sales
 - Gambling winnings
 - Inheritances and gifts
 - Compensation from legal rulings

In higher-risk situations, The Company will periodically request SOF information, even if there has been no change in the customer's activity pattern. This ongoing diligence is essential for proactively addressing any potential concerns.

- *Transaction Purpose:* Ask for information regarding the reasons for intended or performed transactions to ascertain their legitimacy and ensure they align with the customer's profile.
- *Senior Management Approval:* Require approval from senior management before commencing or continuing the business relationship with higher-risk customers.
- *Enhanced Monitoring:* Implement increased scrutiny of the business relationship, which may involve more frequent reviews of transactions and account activities.
- *Account Verification for Initial Payments:* Require that the initial payment is made through an account in the customer's name with a bank that adheres to similar CDD standards.

5.8. ONGOING MONITORING

5.8.1 ONGOING CUSTOMER PROFILE MONITORING

During the periodic review of a customer, The Company verifies and confirms that the CDD information about the client, nature and purpose of the business relationship, and SOF is still accurate and up to date, evaluate if there are external signals (bad press/adverse news,

incidents) that could give rise to a change in the business risk profile of the customer and ensure to perform screening against sanctions lists and PEP lists. The periodic review also includes an overall review of the transaction behavior of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

The periodical review of the customer is based on the risk profile of the customer:

- For high-risk customers - once per year;
- For medium risk customers - once every 2 years;
- For low-risk customers - once every 3 years.

5.8.2 ONGOING TRANSACTION MONITORING

The Company performs both real-time monitoring of transactions, as well as post-event monitoring, to ensure that such transactions and activity are consistent with the Company's knowledge of the client and their expected activity. More attention is paid to high amounts, high-risk clients and high-risk jurisdictions.

Particular risk factors will be closely monitored concerning business relationships and transactions, including:

- Gambling or transaction patterns that diverge from what is considered normal or what the customer initially indicated when establishing the business relationship.
- Execution of unusually large transactions by the customer.
- Requests for withdrawals to accounts other than those verified to belong to the customer (such withdrawals are prohibited).
- Requests to transfer gambling accounts or winnings to third parties (such transfers are also prohibited).

5.9. RELIANCE ON THIRD PARTIES TO PERFORM DUE DILIGENCE

The Company recognizes that when contracting or outsourcing specific functions, there is a risk of increased AML exposure if the third parties involved are not properly vetted and their relevant processes are not assessed. Prior to entering into any service agreements that fall under this Policy, the Company performs due diligence to verify the legitimacy of the potential partners. This due diligence includes, at a minimum, establishing the identity of the party and where it concerns a legal person - of its beneficial owners and the persons authorized to represent it.

Additionally, where applicable, potential third-party suppliers are required to submit a copy of their AML, CTF and CPF policies and procedures, proof of pertinent licensing or certification. The Compliance Officer will review these documents for their accuracy and completeness prior to entering into any agreements.

6. REPORTING OF UNUSUAL TRANSACTIONS

6.1. REPORTING OBLIGATIONS

All unusual activities and transactions, including attempted transactions, are initially reported internally. The officers responsible for transaction monitoring must immediately report any unusual activities to the Compliance Officer upon identification, providing a brief description of the specific mitigating measures taken.

All employees who engage with customers or have access to customer information receive anti- money laundering training. This training prepares them to identify actions by customers that may reasonably raise suspicions of money laundering or terrorism financing. Staff members are expected to recognize and understand any gaming or transaction behaviors that might indicate customer involvement in money laundering or terrorism financing. If they know, suspect, or have reasonable grounds to believe they are dealing with the proceeds of crime, they must submit an Internal Unusual Activity Report to the Compliance Officer (CO) in accordance with the Reporting Procedure. This ensures that the employee's legal obligation to report is fulfilled. Please see [Appendix III](#) for the Report form.

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than 24 hours after the transaction has been executed, using the Internal Unusual Activity Report form. If a more in-depth investigation is necessary, the Compliance Officer will complete this within ten (10) business days. During this time, the Compliance Officer may request additional information from relevant departments.

If the Compliance Officer concludes that the activity is unusual, a report shall be submitted to the FIU Curaçao regarding any unusual monetary operations or transactions within 48 hours. In any cases whereby the report is made under one of the objective indicators, as defined below, the report must be made to the FIU Curaçao no later than 48 hours after the transaction has been executed.

6.2. RECOGNITION OF UNUSUAL TRANSACTIONS

Staff will be trained to recognize unusual transactions based on customer profiles and specific indicators. Reporting procedures to the compliance officer will be established.

In accordance with the NORUT, The Company is observing both objective and subjective indicators to assess whether a customer's transaction is deemed unusual. All such transactions must be reported to the compliance officer in a format approved by management. Additionally, any supporting documentation, such as copies of identification, cash-out slips, and other relevant records, must also be submitted as supplements.

The Compliance Officer is tasked with maintaining an organized filing system for these records. If the Company fails to report internally identified transactions to the FIU, the rationale for this decision must be thoroughly documented and signed by the compliance officer and/or management. In accordance with the FATF Recommendations, the Company and its employees pays particular attention to all complex or unusually large transactions, as well as any unusual transaction patterns that lack a clear economic or legitimate purpose.

The following transactions or intended transactions are deemed unusual:

- a. A transaction, which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism;
- b. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. A transaction amounting to Cg. 5,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner. This includes but is not limited to:
 1. A cashless transaction in the amount of Cg. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Cg. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Cg. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Cg. 5,000.00 or more;
- d. Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Please note that indicators (a) to (c) are referred to as "objective indicators", while (d) is referred to as "subjective indicator". While the objective indicators are based on measurable facts and do not require interpretation automatically classifying a transaction as unusual, the subjective criterion involves a more nuanced assessment, considering the context and behavior of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Cg. 5,000.00 resets per game day of the user.

6.3. PROHIBITION OF DISCLOSURE

All reports and investigations must be handled with the highest level of confidentiality in accordance with Article 20 of NORUT. Unauthorized disclosure of information related to unusual activity reports is strictly prohibited and may lead to legal and disciplinary action.

The Company has implemented a system of measures to ensure that employees and representatives who report suspicions of money laundering, terrorist financing, and/or financing of proliferation to the FIU Curaçao are safeguarded from threats or hostile actions by other employees, members of the management body, or customers. Additionally, they are protected from adverse or discriminatory employment actions.

6.4. RECORD KEEPING

The Company retains all necessary records of transactions, both domestic and international, for a minimum of five (5) years to ensure compliance with information requests from regulatory authorities. These records must be detailed enough to allow for the reconstruction of individual transactions, including the amounts and types of currency involved, if applicable, to provide evidence for potential criminal prosecutions.

All records gathered through CDD measures, such as copies of official identification

documents, account files, and business correspondence, **will** be stored for at least five (5) years after the business relationship has ended or after the date of an occasional transaction.

Records shall be stored in a manner that ensures their integrity, confidentiality, and accessibility. Access is restricted to authorized personnel only. Regular backups of electronic records shall be conducted and stored in a separate, secure location to prevent data loss.

After the retention period, records shall be disposed of securely to prevent unauthorized access or disclosure.

When properly ordered to do so by any enactment, rule of law or court order, the Company shall provide a document, customer due diligence information, or enhanced due diligence information and the Company will maintain a register of the documents and information provided and will keep a copy of the same.

7. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

7.1. APPOINTMENT OF A COMPLIANCE OFFICER

A senior compliance officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our AML compliance officer will have timely access to customer identification data, transaction records, and other relevant information. This officer will operate independently to ensure robust compliance.

7.1.1 DUTIES OF THE COMPLIANCE OFFICER

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the Company's efforts against money laundering and financing of terrorism and financing of proliferation.

7.2. EMPLOYEE SCREENING AND TRAINING PROGRAMS

7.2.1 EMPLOYEE DUE DILIGENCE

Employee due diligence is a process employed to screen employees with the objective of identifying and reducing The Company's exposure to the risks associated with money laundering and terrorism financing. These procedures apply not only to the Company's contractual employees, but also to its contractors and subcontractors.

Any employee whose position may enable them to facilitate ML or TF must undergo screening. This requirement applies to prospective employees prior to their hiring for such roles, as well as current employees from time to time. Regular updates and re-evaluations are essential for maintaining an effective compliance program against ML, TF and **PF**.

To screen both current and potential employees, The Company will:

- Identify the individuals;
- Verify their identity;
- Confirm their employment history, such as through references; and
- Determine their suitability for the position and assess whether they pose any risk to the Company.

Positions that may render an employee vulnerable to collusion with or coercion by criminal organizations should undergo more rigorous checks. The Company must evaluate whether:

- The employee has a criminal record, which may be verified through a police check.
- The employee is or has been subject to regulatory, court, or legal actions.
- The employee has leveraged bankruptcy laws for personal gain.

7.2.2 TRAINING

The company provides AML, CTF, and CPF training based on each employee's role and responsibilities. Training covers what staff need to know and do to meet legal and policy requirements. We keep records of all training

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

Training is updated regularly to reflect changes in laws, regulations, or company policies. Extra training will be given when:

- New rules are introduced
- New products or services change our risk exposure
- A breach happens due to lack of knowledge

7.3. INDEPENDENT AUDIT FUNCTION

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 scope and results must be documented, with any deficiencies reported to senior management, along with requests for prompt corrective actions.

7.4. EXAMINATION BY THE CURAÇAO GAMING AUTHORITY

The Company shall provide information and documentation regarding its money laundering and terrorist financing policies and procedures to examiners of the CGA during examinations or upon request. The following items must at all times be readily available and accessible:

- The written and approved AML Compliance Program addressing ML/TF/PF.
- Records of the Business Risk Assessment.
- The name and job description of the Compliance Officer responsible for the company's AML policies and procedures.
- Records of reported unusual transactions.
- Records of unusual transactions that required further investigation.
- Records of frozen accounts.
- A schedule of training provided to personnel on ML/TF/PF.
- Assessment reports on the company's policies and procedures regarding money laundering, terrorist financing, and proliferation financing from the internal audit department or an external auditor.
- Customer files, including risk assessments, CDD, customer acceptance, and transaction information.

8. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

The company is fully committed to adhering to all applicable laws and regulations related to Anti- Money Laundering (AML), Counter-Terrorism Financing (CTF), and sanctions enforcement as established by the jurisdiction of Curacao, aligning with international best practices, including the FATF Recommendations. Compliance with this Policy is mandatory for all employees, officers, agents, and third-party service providers. Non-compliance may expose the organization and individuals to significant legal, regulatory, and reputational

risks, including fines or penalties imposed by Curacao's authorities, revocation or suspension of the company's gaming license, and potential criminal prosecution for willful violations.

Additionally, non-compliance can lead to reputational damage, resulting in loss of customer trust, negative media exposure, and strained relationships with financial partners. Operational disruptions may also occur, such as freezing of funds, loss of access to financial systems, and increased scrutiny from regulators.

Employees who violate the AML/CTF Policy may face disciplinary actions, including formal warnings, suspension, or termination for serious or repeated breaches, as well as potential referral to law enforcement. Third-party providers may have their agreements terminated if found non-compliant. All employees must understand and comply with the AML/CTF Policy, participate in mandatory training, and report any unusual behavior or breaches to the Compliance Officer, who will ensure that whistleblower protections are in place.

The Compliance Officer and senior management are responsible for investigating violations, determining appropriate disciplinary actions, and reporting serious breaches to relevant authorities. **All** enforcement actions are documented and reviewed periodically to improve the compliance program.

APPENDIX I — RESTRICTED JURISDICTIONS LIST

Effective: 24 March 2026 | Approved by: Emmanuel [Legal], Compliance Officer | Next review: May 2027

The following jurisdictions are restricted. Customers residing in or connecting from these countries or territories are not permitted to register or access financial services on the Company's platform. This list is enforced at onboarding via the country-of-residence drop-down and via IP-based geo-blocking.

Restricted Jurisdiction	Region/Group	Basis for Restriction
NL ANTILLES		
Aruba	NL Antilles	No authorisation / Kingdom territory restriction
Bonaire	NL Antilles	No authorisation / Kingdom territory restriction
Curaçao	NL Antilles	Domestic jurisdiction — operator jurisdiction, not a serviceable market
Saba	NL Antilles	No authorisation / Kingdom territory restriction
Sint Eustatius (Statia)	NL Antilles	No authorisation / Kingdom territory restriction
Sint Maarten	NL Antilles	No authorisation / Kingdom territory restriction
EUROPEAN UNION		
Austria	European Union	No CGA authorisation / regulated market
France	European Union	No CGA authorisation / regulated market
Germany	European Union	No CGA authorisation / regulated market
Greece	European Union	No CGA authorisation / regulated market
Malta	European Union	No CGA authorisation / regulated market
Netherlands	European Union	No CGA authorisation / regulated market
Spain	European Union	No CGA authorisation / regulated market
EUROPE		
United Kingdom	Europe	No CGA authorisation / regulated market
ASIA/PACIFIC		

Australia	Asia/Pacific	No CGA authorisation / local prohibition
NORTH AMERICA		
United States of America	North America	No CGA authorisation / local prohibition
United States Minor Outlying Islands	North America	U.S. territory — same restriction as USA
FRANCE/OVERSEAS		
French Guiana	France/Overseas	French overseas territory — same restriction as France
French Polynesia	France/Overseas	French overseas territory — same restriction as France
French Southern Territories	France/Overseas	French overseas territory — same restriction as France
BRITISH CROWN DEPENDENCY		
Isle of Man	British Crown Dependency	No CGA authorisation / own regulatory regime
FRANCE/OVERSEAS		
Saint Barthélemy	France/Overseas	French overseas collectivity — same restriction as France
Saint Martin (French part)	France/Overseas	French overseas collectivity — same restriction as France
NL ANTILLES		
Sint Maarten (Dutch part)	NL Antilles	Kingdom territory restriction — duplicate entry for drop-down
EUROPE		
United Kingdom (excl. Northern Ireland)	Europe	Sub-designation of UK restriction
United Kingdom of Great Britain and Northern Ireland	Europe	Full designation of UK restriction
BRITISH OVERSEAS TERRITORY		
Virgin Islands (British)	British Overseas Territory	No CGA authorisation
NORTH AMERICA		
Virgin Islands (U.S.)	North America	U.S. territory — same restriction as USA

This list comprises 28 restricted jurisdictions across NL Antilles, European Union/Europe, Asia/Pacific, North America, and French/British overseas territories. It will be reviewed annually by the Compliance Officer and updated to reflect any changes in the Company's licensing position or applicable regulatory guidance.

For any questions regarding this policy, please contact the designated Compliance Officer.