

Approval	Managing Director Gouloud Hammoud obo Guardian Corporation Curaçao B.V.  (signature)
Responsible Office	Compliance Officer
Effective Date	31 January 2026
Next Review Date	31 January 2027

Swivel B.V.

**Anti-Money Laundering, Counter-Terrorism
Financing and Counter-Proliferation Financing
Policy**

Version 1.0

Table of Contents

1. DEFINITIONS.....	5
2. POLICY OVERVIEW.....	8
2.1. POLICY STATEMENT	8
2.2. PURPOSE OF THIS POLICY	8
2.3. AUDIENCE	9
3. POLICY IMPLEMENTATION	9
3.1. GOVERNANCE AND OVERSIGHT	9
3.2. RESPONSIBILITIES OF THE SENIOR MANAGEMENT	10
3.3. COMPLIANCE OFFICER.....	10
3.4. EMPLOYEES	10
3.5. SUPPORTING PROCEDURES AND DEPARTMENTAL OVERSIGHT	11
3.6. REVIEW AND CONTINUOUS IMPROVEMENT.....	11
4. THE RISK-BASED APPROACH	11
4.1. EXPLANATION OF THE RISK-BASED APPROACH.....	11
4.2. BUSINESS RISK ASSESSMENT (BRA)	12
4.3. TECHNOLOGICAL DEVELOPMENTS RISK ASSESSMENT (TDRA)	13
5. CUSTOMER ACCEPTANCE POLICY.....	14
5.1. CUSTOMER RISK ASSESSMENT	14
5.2. PROHIBITED ACCOUNTS.....	15
6. CUSTOMER DUE DILIGENCE (CDD) MEASURES	15
6.1. CUSTOMER DUE DILIGENCE (CDD)	16
6.2. CUSTOMER ONBOARDING AND IDENTIFICATION.....	16
6.3. VERIFICATION OF IDENTITY	16
6.4. VERIFICATION OF BENEFICIAL OWNERSHIP	17
6.5. CUSTOMER RISK ASSESSMENT AND PURPOSE OF RELATIONSHIP	17
6.6. TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS.....	17

6.7.	SIMPLIFIED DUE DILIGENCE (SDD)	18
6.8.	ENHANCED DUE DILIGENCE (EDD)	18
6.9.	POLITICALLY EXPOSED PERSONS (PEPs)	19
6.10.	SANCTIONS SCREENING	20
6.11.	ONGOING MONITORING	20
6.11.1.	<i>Ongoing Customer Profile Monitoring</i>	20
6.11.2.	<i>Ongoing Transaction Monitoring</i>	21
6.12.	PARTNER DUE DILIGENCE	21
6.13.	ADDITIONAL DUE DILIGENCE FOR PAYMENT SERVICE PROVIDERS (PSPs)	22
6.14.	ONGOING MONITORING OF PARTNERS	22
6.15.	RELIANCE ON THIRD PARTIES TO PERFORM DUE DILIGENCE	23
7.	REPORTING OF UNUSUAL TRANSACTIONS	24
7.1.	REPORTING OBLIGATIONS	24
7.2.	RECOGNITION OF UNUSUAL TRANSACTIONS	25
7.3.	PROHIBITION OF DISCLOSURE	25
7.4.	RECORD KEEPING	26
7.4.1.	<i>Retention of Records</i>	26
7.4.2.	<i>Format and Accessibility</i>	26
7.4.3.	<i>Data Protection and Confidentiality</i>	26
7.4.4.	<i>Regulatory and Audit Access</i>	26
8.	TERMINATION OF BUSINESS RELATIONSHIP	27
8.1.	GROUND FOR TERMINATION	27
8.2.	TERMINATION PROCEDURE	27
8.3.	RECORD KEEPING AND RETENTION	28
8.4.	BUSINESS AND COMPLIANCE CONSIDERATIONS	28
9.	ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM	28
9.1.	APPOINTMENT OF A COMPLIANCE OFFICER	28

9.1.1.	<i>Duties of the Compliance Officer</i>	28
9.2.	EMPLOYEE SCREENING AND TRAINING PROGRAMS.....	29
9.2.1.	<i>Employee Due Diligence</i>	29
9.2.2.	<i>Training</i>	30
9.3.	INDEPENDENT AUDIT FUNCTION	30
9.4.	EXAMINATION BY THE CURAÇAO GAMING AUTHORITY.....	30
10.	COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	31
11.	RELATED INFORMATION	31
12.	CONTACT	32
13.	POLICY HISTORY	32

1. Definitions

"CGA"	Curaçao Gaming Authority
"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.
The "Company"	means Swivel B.V. (company number 164460, registered address Kaya Richard J. Beaujon Z/N, Willemstad, Curaçao) which is a holder of license number OGL/2024/634/0590 from the CGA.
"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 traveller'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).
"Payment Service Provider (PSP)"	is any regulated or unregulated third-party entity that provides payment processing or related financial services to the Company, including the processing of deposits, withdrawals, transfers, or other payment transactions on behalf of customers. This includes, but is not limited to, acquiring banks, e-wallet providers, card processors, payment gateways, virtual asset service providers (VASPs), and alternative payment method providers.
"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 NORUT.
"(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 Overview

2.1. Policy Statement

Swivel B.V. (hereinafter the “Company”), is licensed and regulated by Curaçao Gaming Authority (CGA) to offer remote (online) games of chance, under License No. OGL/2024/634/0590. In accordance with applicable legislation and its license conditions, the Company has developed a comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing (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.

2.2. Purpose of this Policy

The purpose of this Policy is to ensure that the Company complies with all applicable AML, CTF and CPF laws and regulations applicable to the Curaçao gaming sector, and to protect the integrity of the Company’s operations.

This Policy establishes the principles and requirements that all employees, contractors and relevant third-party partners must follow in order to prevent the Company’s services from being used for money laundering, terrorist financing or proliferation financing.

This Policy is based on the AML/CTF/CPF framework of Curaçao, including in particular:

- 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 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

These laws and standards oblige the Company to adopt risk-based procedures for customer due diligence, monitoring of transactions, and reporting of unusual activities.

The objectives of this Policy are to:

- ensure that all staff understand and comply with their AML/CTF/CPF obligations;
- prevent the misuse of the Company's platform for criminal or prohibited activities;
- support timely detection and reporting of unusual or suspicious transactions;
- promote a culture of compliance, transparency and accountability throughout the organization.

This Policy also serves to protect the Company's business by:

- safeguarding its reputation with customers, financial institutions and regulators;
- maintaining eligibility for gaming licenses and business partnerships;
- reducing legal, financial and operational risks associated with non-compliance; and
- supporting the long-term continuity and sustainability of the Company's operations.

2.3. Audience

This Policy applies to all personnel, including all employees, officers, directors, contractors, and third parties engaged in business with or for the Company.

3. Policy Implementation

This Policy is implemented through a system of internal controls, defined responsibilities, and documented procedures designed to ensure effective compliance with AML, CTF and CPF requirements and to maintain a safe and compliant gaming environment.

Operational procedures supporting this Policy (including Customer Due Diligence, transaction monitoring, reporting, record keeping and training procedures) are documented separately and are maintained under the oversight of the Compliance Officer.

3.1. Governance and Oversight

Overall responsibility for the implementation of this Policy rests with Senior Management. Day-to-day oversight and execution is delegated to the Compliance Officer, supported by relevant operational departments.

The Company ensures that:

- adequate systems and controls are in place to support compliance;
- sufficient resources, staff and technology are allocated to AML, CTF and CPF functions; and
- employees understand their individual responsibilities under this Policy.

3.2. Responsibilities of the Senior Management

The Senior Management is responsible for:

- approving and endorsing this Policy and its underlying principles;
- appointing the Compliance Officer and defining their authority and responsibilities;
- ensuring effective systems and controls are implemented across the Company;
- ensuring the Compliance Officer has unrestricted access to relevant customer and transaction data;
- ensuring that reporting lines for unusual transactions are clearly communicated to all staff;
- providing adequate resources, staffing and technical tools for AML, CTF and CPF compliance; and
- reviewing annual compliance reports and ensuring that any identified weaknesses are remedied.

3.3. Compliance Officer

The Compliance Officer is responsible for the operational implementation and ongoing monitoring of this Policy.

Key duties include:

- overseeing compliance with AML, CTF and CPF obligations;
- maintaining and updating AML procedures in line with regulatory developments;
- monitoring business and operational risks related to ML, TF and PF;
- supervising customer due diligence, transaction monitoring and reporting processes;
- receiving and assessing internal reports of unusual activity;
- submitting reports to the FIU Curaçao where required;
- coordinating AML training and awareness programs; and
- reporting material findings and compliance issues to Senior Management.

All AML procedures documented separately are subject to the Compliance Officer's oversight.

3.4. Employees

All employees, contractors and relevant third-party partners are required to comply with this Policy and the related procedures applicable to their role.

Employees must:

- follow established customer due diligence and monitoring procedures;
- remain alert to unusual or suspicious behaviour;
- report any unusual activity immediately to the Compliance Officer;
- complete required AML, CTF and CPF training; and
- maintain confidentiality and comply with tipping-off prohibitions.

Failure to comply with this Policy may result in disciplinary action.

3.5. Supporting Procedures and Departmental Oversight

The practical implementation of this Policy is supported by documented procedures, including but not limited to:

- Customer Acceptance and Customer Due Diligence procedures;
- Risk Assessment and Risk-Based Approach procedures;
- Transaction Monitoring procedures;
- Reporting of Unusual Transactions procedures;
- Record Keeping and Data Protection procedures; and
- Affiliate and PSP Due Diligence procedures.

Oversight responsibility:

- Compliance Officer: overall ownership and monitoring of AML procedures;
- Operations / Customer Support: execution of CDD and monitoring procedures;
- IT / Data Management: system support and secure record keeping;
- Human Resources: employee screening and training coordination.

All procedures are reviewed periodically and updated as required to reflect regulatory and business changes.

3.6. Review and Continuous Improvement

The effectiveness of this Policy and its supporting procedures is reviewed on an ongoing basis through:

- internal monitoring by the Compliance Officer;
- independent audit reviews; and
- regulatory examinations by the CGA.

Any identified deficiencies must be documented and corrected promptly. Senior Management remains responsible for ensuring continuous improvement of the AML, CTF and CPF framework.

4. The Risk-Based Approach

4.1. 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 an assessment of the risks associated with ML, TF and PF 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.

4.2. Business Risk Assessment (BRA)

The 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.

The Company applies a structured methodology to assess its exposure to ML, TF and PF risks. Each identified risk factor relating to customers, products and services, geographic exposure, and delivery channels is evaluated using a qualitative risk scoring model.

For each risk factor, the following elements are assessed:

- **Likelihood:** The probability that the identified risk could materialise, taking into account factors such as transaction volumes, customer behaviour patterns, accessibility of products, cross-border exposure, and historical incidents.
- **Impact:** The potential regulatory, financial, operational, and reputational consequences to the Company should the risk materialise, including exposure to sanctions breaches, regulatory enforcement, license impact, and financial loss.

Each risk factor is assigned a rating of Low, Medium or High based on a combined assessment of likelihood and impact.

The Company distinguishes between:

- **Inherent Risk:** The level of risk present before the application of mitigating controls; and
- **Residual Risk:** The level of risk remaining after the application of controls, such as Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), transaction monitoring, sanctions screening, customer limits, product restrictions, and reporting procedures.

Tailored controls and measures are then implemented to address these risks. Residual risk is evaluated to determine whether it falls within the Company's defined risk appetite. Where residual risk exceeds acceptable levels, additional mitigating measures must be implemented or the activity, product, customer segment, or geographic exposure must be restricted or discontinued.

All risk scoring decisions, assumptions, and applied mitigating measures are documented to ensure transparency, auditability, and regulatory review.

BRAs are conducted regularly to maintain an accurate risk profile, with comprehensive assessments performed annually. Additional assessments may be triggered by significant events, such as the introduction of new products, regulatory changes, or major shifts in the business environment. The Board of Directors shall formally approve the BRA and risk appetite.

The Company does not accept customers or business relationships that fall outside its defined risk appetite, including those involving sanctioned jurisdictions or reminder anonymity-enhancing products.

4.3. Technological Developments Risk Assessment (TDRA)

In line with the risk-based approach the Company shall conduct a TDRA in order to mitigate any ML, TF and PF risks. The findings of each TDRA shall be incorporated into the Company's BRA. Where new or increased risks are identified, the relevant risk ratings shall be updated, and the impact on the Company's overall risk profile and defined risk appetite shall be reassessed. Where necessary, additional mitigating controls shall be implemented to ensure residual risk remains within acceptable limits.

Where the Company is considering the implementation of technology, as indicated in the following section, the Compliance Officer shall perform such an assessment when any of the following criteria is being considered:

- The development of a new product;
- A new delivery mechanism;
- A new business practice emerges, in particular every time money and technology come together in a new way, whether that is a new payment channel, a new way to transfer money between services or a change in the payment infrastructure offered by technological developments, and
- A new technology is used to deliver new or old services.

Any such risk assessments and the results thereof shall be duly documented and retained in line with the record retention procedures outlined in this Policy, for a period of five (5) years.

When conducting a TDRA, the following must be addressed, where relevant:

- **Anonymity Risk:** Does the new technology increase the ability for customers to remain anonymous?
- **Cross-Border Exposure:** Does it facilitate international payments, P2P transfers, or multi-jurisdiction access?
- **Licensing/Regulation:** Are third-party providers (e.g., e-wallets) regulated in reputable jurisdictions?
- **Transaction Traceability:** Can the Company maintain a clear audit trail for every transaction?
- **Volume and Velocity Risk:** Can the product allow rapid/frequent transactions that might facilitate layering?
- **Integration with Monitoring:** Can the existing AML software capture and analyse transactions from the new channel?
- **Contingency & Response:** If misuse is detected, can the product be paused or suspended immediately?

- **Periodic Re-assessment:** Review the risk at launch + ninety (90) days, and annually thereafter.

Where the assessment identifies residual risk exceeding the Company's defined risk appetite, launch shall be suspended pending implementation of additional mitigating controls and formal approval by Senior Management.

5. Customer Acceptance Policy

5.1. Customer Risk Assessment

The Customer Risk Assessment procedure is a crucial component of the internal AML, CTF and CPF 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:

- o **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.
- o **Product/Service Risk:** This factor assesses the risks associated with the Company'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.
- o **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 list of high-risk jurisdictions subject to Call for Action, FATF list of jurisdictions under increased monitoring, countries on the CFATF Public Statement, OFAC Sanctions Lists and Kingdom Sanction Act Decrees, 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. The company maintains and consistently updates an internal High Risk Country List.

- o **Delivery Channel Risk:** This involves evaluating the methods used to establish a business relationship or conduct transactions. Channels that favour 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 risk** customers will require additional information and documentation in accordance with the Company's policies.
- Accounts classified as **high risk** or displaying potentially suspicious behaviour will be reviewed by compliance personnel and reported to the Compliance Officer (CO) for further investigation. In line with this Policy, certain categories of high risk customers must be subject to Management approval for the establishment and continuation of the business relationship.

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, CTF and CPF compliance program.

5.2. Prohibited Accounts

The Company's Customer Acceptance Policy is formulated in accordance with legal requirements and aligns with the Company's risk appetite as well as the BRA. Therefore, certain categories of individuals are prohibited from being accepted as customers, either by preventing them from registering or by blocking their access to our site, as necessary:

- Individuals under the age of 18.
- Individuals listed on sanctions imposed by 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 who are barred from our websites or included in any national self-exclusion registers as stipulated by licensing conditions.
- Individuals who have submitted documents or information that the Company has reasonable grounds to suspect are fraudulent or falsified.

6. Customer Due Diligence (CDD) Measures

The Company applies a structured and risk-sensitive Customer Due Diligence (CDD) process, beginning at the onboarding stage and continuing throughout the customer relationship. This framework ensures that the Company understands who its customers are, assesses the risk they pose, and applies appropriate verification and monitoring measures in line with Curaçao's AML, CTF and CPF requirements under the NOIS and the NORUT.

All customers are onboarded remotely. As such, identification and verification must take into account the specific risks associated with non-face-to-face business relationships.

The Company prohibits anonymous and fictitious accounts and applies robust internal controls to prevent their creation.

6.1. Customer Due Diligence (CDD)

CDD must be performed:

- When the customer reaches the Cg. 4,000 thresholds (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.

6.2. Customer Onboarding and Identification

At the time of registration, all customers must provide:

- Full name;
- Date of birth;
- Permanent residential address;
- Place of birth;
- Nationality; and
- Identification number.

Customers must verify their identity using reliable, government-issued identification documents such as passport, ID card, or driver's license. The document must be valid, include a photograph, and be legible. If the document is not in a language understood by the Company, a certified translation may be required.

Before accepting the identification document, the Company must validate that the document is genuine and has not been altered or misused.

Validation may include one or more of the following methods:

- Automated document authentication software (security feature checks, template comparison, hologram or microprint detection where applicable);
- Verification of document data against reliable databases or official records where available;
- QR code or machine-readable zone (MRZ) verification (where accessible);
- Certified copies where applicable.

Proof of permanent residential address must be submitted and dated within the last six (6) months (e.g., utility bill or bank statement).

6.3. Verification of Identity

The Company must verify that the person opening the account is the same person shown on the identification document.

Remote verification may include:

- Facial recognition matching between the uploaded document photo and a live image;
- Liveness detection checks to confirm the person is physically present during verification;
- Video-based verification (attended or unattended);
- Biometric matching using reliable and tested algorithms.

Where automated onboarding solutions are used:

- Images and/or video must be captured in real time;
- Image quality must be sufficient to clearly identify the individual;
- Liveness detection must be performed;
- The onboarding process must stop if technical interruptions or poor-quality images prevent reliable verification.

If the system does not provide sufficient confidence in the identity match, additional verification steps must be applied or the onboarding must be escalated for manual review.

All identification data, validation results, biometric checks (where used), and related logs must be retained for at least five (5) years in accordance with record retention requirements.

6.4. 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 behaviour.
- Immediate verification upon withdrawal requests or Cg. 4,000 thresholds.

6.5. 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., payslips, bank statements, tax returns) is required.

6.6. Timeline for Compliance and Non-Compliant Documents

If the customer cannot provide compliant documents within thirty (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 CDD 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.

6.7. 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 SDD:

- 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 behaviour arises, SDD must be upgraded to regular CDD or EDD.

6.8. 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-Favouring 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.

6.9. 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, analysing their spending patterns to ensure they align with declared legal sources of funds.

6.10. 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.

6.11. Ongoing Monitoring

6.11.1. Ongoing Customer Profile Monitoring

The Company conducts ongoing customer profile monitoring on a continuous basis throughout the entire business relationship, combining periodic reviews with event-driven reviews and real-time monitoring controls.

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, checks whether identification documents remain valid 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 behaviour of the client to determine if unusual activities have taken place, for instance in case of transactions which normally would not be expected.

In addition to the scheduled periodic reviews, the Company performs event-driven reviews, including but not limited to:

- at the time of withdrawal requests;
- when transaction monitoring systems generate alerts or predefined internal risk triggers are activated;
- upon significant changes to customer information (e.g., change of address, payment method, occupation, or device);
- upon expiration or replacement of identification documents;

- where adverse media, sanctions or PEP screening results indicate new or increased risk;
- where unusual or suspicious behaviour is detected.

Such event-driven reviews may result in updated risk classification, application of additional CDD or EDD measures, temporary restrictions, or escalation to the Compliance Officer, as appropriate.

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

- High-risk customers – once per year;
- Medium risk customers – once every 2 years;
- Low-risk customers – once every 3 years.

6.11.2. 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).

6.12. Partner Due Diligence

For the purposes of this Policy, "Partner" means any third-party natural or legal person that maintains a contractual or commercial relationship with the Company in connection with its gaming operations, including but not limited to Affiliates, Payment Service Providers (PSPs), marketing partners, technology providers, outsourced service providers, and other business intermediaries.

All Partners are subject to risk-based due diligence, sanctions screening, ongoing monitoring, and appropriate contractual safeguards prior to engagement and throughout the relationship.

The Company remains responsible for ensuring that its partnerships do not expose it to unacceptable ML/TF/PF or sanctions risk.

Before entering into a contractual relationship, the Company shall:

- Assess the nature of the services provided and the associated AML/CFT/CPF risk;
- Consider the Partner's jurisdiction of incorporation and operation;
- Assess whether the Partner will:
 - Handle player funds;
 - Generate player traffic;

- Have access to customer data;
- Perform CDD or onboarding functions.

Partners shall be classified as Low, Medium or High risk. Enhanced due diligence shall apply where higher risk is identified.

Before onboarding any Partner, the Company shall obtain and verify:

- **Corporate Information:**
 - Certificate of Incorporation or Registration;
 - Recent extract from commercial registry (not older than 6 months);
 - Registered address and principal place of business;
 - Details of directors and authorised signatories.
- **Ownership and Control:**
 - Identification of Ultimate Beneficial Owners (natural persons owning or controlling 25% or more, or otherwise exercising control);
 - Identification documents of UBOs and directors;
 - Ownership structure chart (where applicable).
- **Screening and Background Checks:**
 - Sanctions screening of the entity and associated individuals;
 - PEP screening;
 - Adverse media screening;
 - Assessment of country risk (including FATF high-risk or sanctioned jurisdictions). Partners based in sanctioned jurisdictions or jurisdictions subject to FATF Call for Action shall not be engaged.

6.13. Additional Due Diligence for Payment Service Providers (PSPs)

Given the elevated ML/TF/PF risk associated with payment flows, PSPs are subject to enhanced requirements.

In addition to the standard due diligence above, the Company shall obtain and verify:

- Proof of regulatory license or authorization;
- Name of supervisory authority;
- Confirmation of AML/CFT regulatory oversight;
- Description or summary of the PSP's AML framework;
- Confirmation of sanctions screening and transaction monitoring processes;
- Confirmation that transaction data can be provided in a format compatible with the Company's monitoring systems;
- Confirmation of jurisdictions from which payment processing will occur.

Unregulated PSPs, PSPs based in high-risk jurisdictions, or PSPs using complex payment chains require approval by the Compliance Officer and Senior Management prior to engagement.

6.14. Ongoing Monitoring of Partners

The Company shall conduct ongoing monitoring of Partners proportionate to risk level, including:

- Periodic sanctions and PEP re-screening;

- Annual confirmation of corporate and licensing status (for regulated entities);
- Review of jurisdictional exposure;
- Monitoring of traffic sources (for Affiliates);
- Review of payment flow trends and geographic anomalies (for PSPs).

High-risk Partners shall be reviewed at least annually.

Where a Partner appears on a sanctions list, is associated with adverse media involving financial crime, operates in prohibited jurisdictions, fails to provide requested documentation, or is linked to suspicious activity patterns, the matter shall be escalated to the Compliance Officer. The Company may suspend cooperation, withhold payments, conduct enhanced review, terminate the relationship, or report to competent authorities where required.

6.15. Reliance on Third Parties to Perform Due Diligence

The Company may rely on a third party to perform certain elements of Customer Due Diligence (CDD), namely:

- identifying the customer and verifying the customer's identity;
- identifying and verifying the beneficial owner;
- obtaining information on the purpose and intended nature of the business relationship.

Reliance on a third party is permitted only where all regulatory conditions are met and where such reliance is appropriate in light of the Company's risk assessment.

The Company remains ultimately responsible for compliance with all CDD obligations, even where reliance is placed on a third party.

Reliance may only be placed on a third party where the following conditions are satisfied:

- **Immediate Access to CDD Information:** The Company must obtain, without delay, all relevant CDD information collected by the third party relating to:
 - customer identification;
 - beneficial ownership;
 - purpose and intended nature of the relationship.

Employees must ensure that sufficient information is received before establishing or continuing the business relationship.

- **Written Agreement and Access to Documentation:** A written agreement must be in place with the third party providing that:
 - copies of identification documents and CDD records will be made available upon request without delay;
 - records will be retained in accordance with applicable legal requirements;
 - the Company has the right to test and verify that this arrangement operates effectively.

The Compliance Officer shall periodically test this arrangement to confirm that documentation can be obtained promptly and completely.

- **Regulatory Status and AML Controls of the Third Party:** Before relying on a third party, the Company must satisfy itself that the third party:
 - is regulated, supervised, or monitored for AML/CFT/CPF compliance;
 - is subject to CDD and record-keeping requirements equivalent to those applicable to the Company;
 - applies its own independent CDD procedures;
 - has an existing business relationship with the customer that is independent of the relationship to be formed with the Company.

Reliance is not permitted where these conditions cannot be demonstrated.

- **Country Risk Assessment:** The Company must consider the country in which the third party is established. Reliance is not permitted where the third party is based in a jurisdiction:
 - subject to sanctions;
 - identified as high-risk by the FATF;
 - with materially deficient AML supervision.

Country risk must be assessed as part of the Company's Business Risk Assessment.

7. Reporting of Unusual Transactions

7.1. 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 behaviours 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. This ensures that the employee's legal obligation to report is fulfilled.

Employees are required to report any unusual activity to the Compliance Officer immediately, but no later than twenty-four (24) hours after the transaction has been executed. 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 forty-eight (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 forty-eight (48) hours after the transaction has been executed.

7.2. 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 FATF Recommendations, the Company and its employees pay 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 of 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 Gf. 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 Gf. 5,000.00 or more.
 2. Accepting or releasing a deposit in the amount of Gf. 5,000.00 or more at the request of the customer;
 3. Sale to a customer of chips in the amount of Gf. 5,000.00 or more. "Chips" include but is not limited to tokens and credits.
 4. A cash out in the amount of Gf. 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 behaviour of the client. For the purposes of reporting unusual transactions under the objective indicators above, it is noted that the threshold of Gf. 5,000.00 resets per game day of the user.

Additionally, linked transactions that cumulatively reach or exceed Gf. 5,000 within a 24-hour period are considered for unusual transaction reporting in accordance with the Ministerial Decree on Indicators for Unusual Transactions (2015, no. 73).

7.3. 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.

7.4. Record Keeping

The Company maintains a comprehensive record-keeping and data storage system to ensure compliance with the NORUT, NOIS, the Sanctions National Ordinance, the Kingdom Sanctions Act, and the CGA license conditions.

7.4.1. Retention of Records

All CDD documents, including identification records, beneficial ownership information, account files, and related correspondence, are retained for at least five (5) years after the end of the business relationship or the completion of an occasional transaction, whichever is later.

Transaction records, both domestic and international, including deposits, withdrawals, wagers, wins, and transfers, are maintained for a minimum of five (5) years to allow the reconstruction of individual transactions for regulatory and law enforcement purposes.

Unusual transaction reports (UTRs), internal investigation notes, and any supporting documentation submitted to the FIU Curaçao via the goAML portal are retained for a minimum of five (5) years from the date of reporting.

Training records, compliance program reviews, risk assessments, and internal/external audit reports are also retained for five (5) years, as required by the CGA.

7.4.2. Format and Accessibility

Records are kept electronically in secure databases and/or in physical storage, organized to allow prompt retrieval upon request by the CGA, FIU Curaçao, or law enforcement authorities.

Electronic records are regularly backed up and stored in encrypted form with strict access controls limited to authorized compliance personnel.

7.4.3. Data Protection and Confidentiality

Records are treated as confidential and protected from unauthorized access, alteration, or destruction in accordance with Curaçao data protection principles.

Only the Compliance Officer and designated compliance staff may access CDD and transaction data.

Upon the expiration of the retention period, records are securely destroyed in a manner that ensures they cannot be reconstructed.

7.4.4. Regulatory and Audit Access

Records will be made available to the CGA, FIU Curaçao, or any competent authority upon request, in accordance with Article 11 of NORUT and the CGA license conditions.

A log of all disclosures to regulators or law enforcement is maintained for five (5) years.

8. Termination of Business Relationship

The Company may terminate a business relationship with a player where continuation would violate law, present unacceptable risk, or is otherwise necessary to protect the player or the integrity of the platform. Termination aligns with Curaçao AML, CTF and CPF obligations, the Player Complaints Policy of the Company, and the Responsible Gaming Policy.

8.1. Grounds for Termination

- **Regulatory and AML Grounds**
 - Incomplete or failed CDD/EDD verification under NOIS/NORUT.
 - Suspicion of money laundering, terrorist financing, or proliferation financing, supported by an internal UTR to FIU Curaçao.
 - Customer appears on sanctions lists under the Sanctions National Ordinance or Kingdom Sanctions Act.
- **Responsible Gaming and Player Protection**
 - Player is a minor or a vulnerable person per LOK Article 1.1(h).
 - Player triggers self-exclusion or operator-initiated exclusion under the Responsible Gaming Policy.
 - Player exhibits problematic gambling behaviour, or continued access poses risk to the player or others
- **Breach of Terms or Fraud**
 - Player engages in fraud, collusion, bonus abuse, or third-party account use.
 - Player violates civil or criminal law, or uses the account for unlawful purposes

8.2. Termination Procedure

- **Internal Review and Approval**
 - Compliance Officer documents reason and supporting evidence.
 - High-risk or regulatory closures require management approval.
- **Account Actions**
 - Account is suspended immediately.
 - Balances are refunded to the original payment method within two business days, unless funds are frozen per AML or FIU directive.
 - Player is removed from all marketing lists.
- **Regulatory Reporting**
 - All AML-related terminations that involve suspicious or unusual activity are reported to FIU Curaçao via goAML.
 - The CGA is not notified of routine account terminations. Notification will only occur where the termination forms part of a reportable incident, a regulatory request, or a compliance audit requiring disclosure, in accordance with the B2C License Conditions and the LOK.
- **Player Notification and Tipping-Off**
 - Account termination is always assessed against the tipping-off prohibition under NORUT Article 12.

- Decision Process:
 - Compliance Officer evaluates whether notifying the player could alert them to an AML investigation or FIU report.
 - If notification poses a tipping-off risk, communication is delayed or omitted, and only operational messages (e.g., “account closed per terms”) are sent.
 - Documentation of the rationale is mandatory and retained in the compliance file.

8.3. Record Keeping and Retention

Termination records must always include KYC/CDD/EDD documents, reason for termination and supporting evidence, copies of FIU reports (if any), internal approvals or communications. Records are retained for five (5) years or seven (7) years if related to self-exclusion.

8.4. Business and Compliance Considerations

All business and compliance measures following account termination are carried out in strict adherence to AML regulations and internal controls. Any player funds that are frozen are managed exclusively in accordance with the instructions of the FIU Curaçao and the applicable AML laws.

Following the closure of an account, the Company actively monitors linked accounts, associated devices, and access points to prevent any attempt at circumvention or unauthorized re-registration.

All account terminations are executed in alignment with the Player Complaints Policy and the Responsible Gaming Policy. Players retain the right to file complaints or escalate to Alternative Dispute Resolution (ADR) if they believe a closure was unfair, unless such communication is restricted under the tipping-off provisions of the NORUT.

9. Anti-Money Laundering Compliance Program

9.1. Appointment of a Compliance Officer

A Compliance Officer will be designated, separate from our gaming operations, responsible for overseeing the AML program and ensuring compliance with regulations. Our 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.

9.1.1. 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 analyse 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.

9.2. Employee Screening and Training Programs

9.2.1. 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;
- Screen them against sanctions and PEP lists;
- 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. Risk increasing factors related to the employee (e.g. country of origin, country of residence, PEP or RCA status, inconsistencies in their profile and work history, etc.) also subject the employee to enhanced onboarding and ongoing checks performed by the Compliance Officer. 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.

9.2.2. 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

9.3. 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.

9.4. 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.

10. Compliance and Consequences of Non-Compliance

The Company is fully committed to adhering to all applicable laws and regulations related to AML, CTF and CPF 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 operational license, and potential criminal prosecution for wilful 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 this 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 and CPF Policy, participate in mandatory training, and report any unusual behaviour 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.

11. Related Information

- Responsible Gaming Policy
- Player Complaints Policy
- Information Security Policy

12.Contact

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

13.Policy History

Date	Version	Summary Changes
31 January 2026	1.0	Policy implementation