

Anti-Money Laundering Policy

Topc B.V.

(A company registered in Curaçao with registration number
163568)

Registered Office: Korporaalweg 10, Curaçao

Version 3.0

Effective Date: 20.07.2025

1. Policy Statement

Topc B.V., the company registered in Curaçao, with its company number 163568, with registered office at Korporaalweg 10, Curacao (hereinafter referred to as the “Company”, “we”, “us”, or “our”), is fully committed to the prevention of money laundering, terrorist financing, and the proliferation of weapons of mass destruction. This Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy outlines our intent, scope, and approach to ensuring compliance with all relevant legal and regulatory obligations applicable to the gaming sector in Curaçao.

As of February 15, 2019, the Curaçao Gaming Control Board (GCB) was officially appointed as the supervisory authority for AML/CTF compliance in the gaming industry, retroactively effective from January 1, 2016. In accordance with this regulatory framework, we strictly adhere to the provisions outlined in the National Ordinance on the Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, the Kingdom Sanction Act, and the related national decrees, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction.

This Policy applies to all of our gaming operations, including online gaming services, and mandates the implementation of robust internal procedures such as CDD, ongoing monitoring, and the reporting of unusual transactions. It is aligned with the FATF Recommendations, as Curaçao is a member of the Caribbean Financial Action Task Force (CFATF), supporting effective international efforts to combat financial crimes.

The Company is fully aware that non-compliance with AML/CTF laws and regulations may lead to administrative and criminal sanctions. Therefore, we are committed to maintaining a culture of compliance and integrity, ensuring that all our employees, systems, and processes meet the required standards set forth by the GCB and relevant international obligations.

2. Purpose

The purpose of this Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy is to establish a comprehensive framework for preventing the misuse of the Company's services for money laundering, terrorist financing, and the proliferation of weapons of mass destruction.

By implementing strict internal controls, risk-based procedures, and CDD measures, we aim to detect, deter, and report any suspicious activities in accordance with the applicable laws of Curaçao and international standards.

This Policy also promotes awareness and accountability among employees and partners, ensuring that everyone involved in our business understands their responsibilities in identifying and responding to potential threats related to money laundering or terrorist financing.

3. Audience

This AML/CTF Policy applies to all individuals and entities involved in the operations of the Company. The following stakeholders are required to understand and comply with the provisions of this Policy:

- **All employees**, including full-time, part-time, and temporary staff, regardless of their role or seniority level.
- **Management and executive leadership**, who are responsible for setting the tone at the top and ensuring effective implementation of AML/CTF measures.
- **Subcontractors and consultants** who perform services on behalf of the Company and may have access to customer data or financial transactions.
- **Third-party suppliers and service providers**, particularly those involved in payment processing, customer verification, or other risk-sensitive operations.
- **Any other individuals or entities acting under the authority or on behalf of the Company**, in any capacity that could expose the Company to money laundering or terrorist financing risks.

All relevant stakeholders must be familiar with the AML/CTF requirements and participate in ongoing training and compliance initiatives as mandated by the Company.

4. Definitions

The following definitions apply specifically within the context of this Policy:

- **Anti-Money Laundering (AML)** – a set of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income within the online gaming environment.
- **CFATF (Caribbean Financial Action Task Force)** – a regional organization of twenty-four (24) states in the Caribbean Basin, Central and South America. Member states, including Curaçao, have committed to implementing common countermeasures to combat money laundering and terrorist financing.
- **Compliance Officer** – a senior management-level individual, independent from day-to-day operations, appointed by the Company to oversee the implementation of AML/CTF controls and to ensure effective detection and prevention of money laundering and terrorist financing.
- **Customer Due Diligence (CDD)** – the standard process of collecting and verifying information about a customer's identity, financial activities, and risk profile before allowing them to participate in gaming activities.
- **Enhanced Due Diligence (EDD)** – additional, more rigorous checks performed on customers who present a higher risk (e.g., Politically Exposed Persons or those with large or unusual transactions), including deeper investigation into the source of funds and wealth.
- **FATF (Financial Action Task Force)** – an international intergovernmental body established in 1989. FATF develops and promotes global standards and policies to protect the financial system from money laundering, terrorist financing, and the financing of the proliferation of weapons of mass destruction.
- **FATF Recommendations** – a set of globally accepted guidelines issued by the FATF. These recommendations serve as a foundation for the Company's internal policies and procedures aimed at combating money laundering, terrorist financing, and related threats.
- **FIU (Financial Intelligence Unit Curaçao)** – the national authority responsible for receiving, analyzing, and reporting unusual transaction reports, as defined in Article 2 of the NORUT. The Company reports all relevant suspicious activity to the FIU in compliance with applicable law.
- **Financing of proliferation (FP)** – 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.
- **Financial Transactions:**
 - For online operations: includes player deposits and withdrawals. Bonuses are excluded. Wagers and winnings are considered gambling transactions and are not classified as financial transactions under this Policy.
- **Kingdom Sanctions Act** – refers to the National Ordinance published under N.G. 2016 no. 54, which provides the legal basis for implementing international sanctions within the Kingdom of the Netherlands, including Curaçao.
- **Know Your Customer (KYC)** – the process by which a gaming operator verifies the identity of its customers, assesses their suitability, and understands the nature of their activities to prevent fraud and money laundering.
- **NOIS (National Ordinance on Identification when Rendering Services)** – the legal framework (N.G. 2017, no. 92) that mandates the Company to identify and verify the identity of clients prior to the provision of services.
- **NORUT (National Ordinance on the Reporting of Unusual Transactions)** – the legal requirement (N.G. 2017, no. 99) under which the Company must report certain transactions to the FIU based on specific indicators of unusual or suspicious activity.
- **Other Online Games** – includes all Company-offered online games beyond traditional casino games, such as sports betting, esports betting, fantasy sports, lotteries, bingo, skill-based games, and virtual sports.
- **Politically Exposed Persons (PEPs):**
 - *Foreign PEPs*: individuals entrusted with prominent public functions by a foreign country, including heads of state, senior politicians, military officials, and their close associates or family members.
 - *Domestic PEPs*: individuals holding similar positions within Curaçao or the Kingdom of the Netherlands.
 - *International Organization PEPs*: individuals who hold senior roles within international organizations (e.g., directors or board members).

• **Risk-Based Approach (RBA)** – a methodology where resources and controls are allocated according to the assessed risk level of customers, products, and transactions, allowing for more intensive scrutiny where the risk of money laundering is higher.

• **Sanctions National Ordinance** – refers to the national legislation published under N.G. 2014 no. 55, mandating compliance with international sanctions adopted by Curaçao.

• **Source of Funds** – the specific origin of the money used for a particular transaction by a customer, such as income, gambling winnings, property sale proceeds, savings, or legal compensation.

• **Source of Wealth** – the broader origin of a customer's overall accumulated wealth over time, including employment history, investments, inheritances, or business ownership.

• **Suspicious Activity Report (SAR)** – a formal report submitted to regulatory authorities when a gaming operator detects activities or transactions that may be linked to money laundering or other financial crimes.

• **(Ultimate) Beneficial Ownership (UBO)** – refers to the natural person(s) who ultimately own or control a customer or who benefit from a transaction. This includes individuals who exercise effective control over a legal entity, even if not directly listed as owners.

• **Unusual Transaction** – a transaction identified as unusual based on pre-defined indicators. Such transactions are subject to enhanced scrutiny and reporting obligations.

• **Weapons of Mass Destruction (WMD)** – a category of weapons designed to cause widespread harm and destruction, primarily encompassing nuclear, chemical, and biological weapons.

5. Policy Implementation

This section outlines how the Company's AML/CTF Policy will be executed in practice, including the allocation of key responsibilities, procedures, and oversight mechanisms.

The Company shall formally designate a **Compliance Officer** who is independent from day-to-day gaming operations. The Compliance Officer will be responsible for the implementation, oversight, and continuous improvement of the AML/CTF program.

The Compliance Officer's responsibilities shall be formally documented in a signed and dated job description indicating their acceptance of the role.

5.1 Business Risk Assessment

The **Business Risk Assessment (BRA)** is a core element of this approach and is designed to ensure that our policies, controls, and procedures are effectively aligned with the specific risks to which the Company is exposed.

Objective and Scope

The purpose of the BRA is to systematically evaluate the ways in which the Company's services, products, delivery channels, jurisdictions, and business relationships could be exploited for ML/TF activities. This assessment enables the Company to:

- Understand its exposure to ML/TF risks.
- Establish a defined risk appetite and tolerance level.
- Apply proportionate and targeted controls based on the identified level of risk (low, medium, high).
- Continuously adapt our AML/CTF measures in line with emerging threats and changing regulatory expectations.

Key Risk Areas Assessed

The BRA covers, but is not limited to, the following factors:

- **Customer profiles** (e.g., PEPs, high-net-worth individuals, non-face-to-face players).
- **Products and services offered**, including their inherent risk for misuse.
- **Payment and transaction methods**, especially high-volume or anonymous transactions.
- **Delivery channels**, particularly online or remote onboarding without physical verification.
- **Geographical exposure**, focusing on high-risk jurisdictions or countries with weak AML regimes.

- **Business partnerships and counterparties**, such as payment processors, affiliates, and service providers.

Risk Assessment Methodology

The Company applies a structured and documented methodology to classify risks as **low, medium, or high**, based on qualitative and quantitative factors. The reasons for each classification are recorded, and credible information sources (e.g., FATF mutual evaluation reports, public advisories, internal transaction monitoring data) are used to support our evaluations.

Review and Ongoing Monitoring

The BRA is reviewed:

- **Annually**, as a minimum requirement, or
- **Immediately**, in response to significant changes in the Company's operations, regulatory obligations, products, markets, or the global AML/CTF environment (e.g., launch of new payment methods, entry into new jurisdictions, changes in laws or sanctions regimes).

Monitoring the effectiveness of risk mitigation measures is continuous. Where deficiencies or heightened threats are identified, control measures are strengthened accordingly.

The Company recognizes that risk is not static and will remain vigilant in updating its risk assessments and controls to remain compliant, adaptive, and resilient in the fight against financial crime.

5.2 Customer Risk Assessment (CRA)

The Company implements a Customer Risk Assessment (CRA) framework to evaluate the specific AML, TF, and PF risks posed by each player. This assessment is crucial for developing a risk-based CDD approach and is conducted at the start of any business relationship or before carrying out an occasional transaction.

Purpose of the CRA

The CRA enables the Company to:

Identify and assess ML/TF/PF risks associated with individual customers;

Create a risk profile for each player (low, medium, or high risk);

Apply proportionate CDD measures in accordance with the Customer Acceptance Policy (CAP);

Ensure continuous monitoring of high-risk customer relationships.

Key Risk Areas Assessed

The CRA evaluates four core risk categories, which are also reflected in the Business Risk Assessment (BRA):

1. Customer Risk

This relates to the intrinsic risk a player poses due to their characteristics, source of funds, or activity patterns. Higher-risk indicators include:

PEPs;

High spenders with no clear source of wealth;

Casual players (e.g., tourists) with sudden or unexplained changes in betting patterns;

Customers using multiple player accounts or unknown third parties;

Junkets or third-party facilitators involved in gaming on behalf of others;

Depositing large sums and quickly withdrawing without significant gameplay

Players with **minimal betting activity** compared to the amount deposited

The Company establishes transaction value thresholds to differentiate between typical and atypical behavior and closely monitors any deviations from standard patterns.

2. Geographical Risk

This assesses the risk posed by a player's location or the origin of their funds. Higher geographical risk exists where customers are:

From countries with weak AML/CTF regimes;

Linked to jurisdictions on FATF, CFATF, OFAC, or U.S. Department of State risk lists;

Associated with countries with high levels of corruption or terrorism financing;

Born in, residing in, or operating from high-risk jurisdictions.

The Company maintains and regularly updates a list of high- and low-risk countries using credible sources (e.g., FATF, Transparency International).

3. Product, Service, and Transaction Risk

Certain casino products and transaction types may inherently carry higher risk, including:

Use of anonymous instruments (e.g., crypto);

Transactions involving peer-to-peer gaming or platform sharing with other operators;

Depositing and withdrawing without actual gameplay;

Use of third-party or stolen financial instruments;

Transactions using multiple payment methods or accounts.

The Company regularly assesses its gaming products, financial services, and payment instruments to evaluate risk levels and identify cases requiring enhanced monitoring.

5.3 Customer Acceptance Policy (CAP)

The Customer Acceptance Policy (CAP) outlines the conditions under which the Company enters into or maintains a business relationship with players. It operates in conjunction with the Customer Risk Assessment (CRA) to ensure a RBA to managing player onboarding and engagement.

The CAP supports the Company's compliance with its Anti-Money Laundering, Countering the Financing of Terrorism (AML/CFT), and Counter-Proliferation Financing obligations. It ensures that all customers are assessed consistently and proportionately in line with the level of ML/TF/PF risk they present.

The CAP has the following primary objectives:

- To ensure customers posing a higher-than-average ML/TF/PF risk are identified and subject to enhanced scrutiny;
- To categorize customers according to risk (low, medium, high);
- To determine and apply the appropriate level of **CDD**;
- To implement procedures for refusing or terminating relationships with unacceptable risk;
- To comply with regulatory requirements related to **PEPs** and **Sanctions Screening**;
- To align customer onboarding practices with the Company's **risk appetite** and regulatory environment.

The Company classifies customers into the following risk tiers, each of which requires a specific level of CDD:

Low Risk

Customers with:

- Low transaction volumes;

- Transparent and consistent behavior.

CDD Measures:

- Standard CDD at onboarding;
- Routine monitoring of transactional behavior;
- Periodic review in line with regulatory timelines.

Medium Risk

Customers with:

- Moderate or increasing transaction volumes;
- Irregular gambling patterns or cross-border activity
- Frequent use of anonymous payment methods

CDD Measures:

- Enhanced verification;
- More frequent transactional reviews;
- Ongoing due diligence and monitoring triggers.

High Risk

Customers with:

- PEP status or close associations with PEPs;
- Residency or origin in high-risk jurisdictions;
- Unusual or unexplained betting behavior;
- Signs of structuring, anonymity, or third-party interactions.

CDD Measures:

- EDD, including detailed scrutiny of source of wealth;
- Senior management approval required to onboard or retain;
- Transaction monitoring on a continuous basis;
- Periodic reassessment based on player activity and regulatory changes.

The Company reserves the right to refuse or terminate service under the following circumstances:

- The customer fails to provide satisfactory identification or CDD documentation;
- The customer is identified on a sanctions list or linked to a terrorist organization;
- The customer is non-cooperative or provides misleading information;
- The risk profile exceeds the Company's established risk appetite;
- The customer is associated with illegal activities or attempted ML/TF/PF.

PEPs and Sanctions Screening

In accordance with AML/CFT requirements, the CAP includes:

- **Mandatory screening** for all customers against PEP and sanctions databases at onboarding and regularly thereafter;
- Enhanced CDD and ongoing monitoring for identified PEPs and their close associates or family members;
- Immediate review and reporting obligations in the event a match is found with:
 - United Nations Sanctions Lists;
 - OFAC, EU, and other relevant bodies' lists;

Local regulatory or law enforcement watchlists

5.4 CDD

CDD is a cornerstone of the Company's AML/CFT/CPF framework. It ensures the identification and verification of customers, ongoing monitoring of business relationships, and detection of suspicious behavior, with the ultimate goal of preventing money laundering, terrorist financing, and proliferation financing.

Casinos are **prohibited from keeping anonymous or fictitious accounts**. The Company shall not establish or maintain a business relationship without first conducting proper CDD. No occasional or ongoing transaction may be permitted without sufficient information about the customer's identity and risk profile.

5.4.1 When CDD Measures Are Required

The Company undertakes CDD in the following scenarios:

- a. When a player engages in a transaction equal to or above **NAf 4,000** (or equivalent in another currency);
- b. When carrying out occasional transactions above **NAf 4,000**, including linked transactions which cumulatively exceed the threshold;
- c. When there is a **suspicion of money laundering, terrorist financing, or proliferation financing**;
- d. When the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

Occasional transactions are typically associated with one-off interactions, especially in land-based settings, but are applicable to online operations when no formal account is opened.

5.4.2 Core CDD Measures

CDD comprises the following components:

a. Identification of the Player

- Required minimum information:
 - Full name
 - Permanent residential address
 - Date of birth
 - Place of birth
 - Nationality
 - Government-issued ID number

In **low-risk cases**, only the name, address, and date of birth may be collected. In **high-risk cases**, additional identifying data may be required.

b. Verification of the Player's Identity

- Must be based on reliable and independent documents, including:
 - Government-issued ID (passport, national ID)
 - Proof of address (bank statement, utility bill, letter from public authority, not older than 6 months)
- Supplementary methods:
 - Email/phone verification
 - Biometric checks
 - IP address and geo-location data
 - Social media or public registries
 - Cross-checks using internal and external databases

c. Understanding the Nature and Purpose of the Business Relationship

- A clear risk-based profile must be developed, considering:

- Stated purpose (e.g. gaming entertainment);
- Expected activity levels;
- **Source of wealth** and **source of funds**, particularly in high-risk scenarios;
- Information may be supplemented by:
 - Income declarations
 - Publicly available data (e.g. Transparency International, KnowYourCountry.com)
 - Statistical data on average income in the jurisdiction

d. Ongoing Due Diligence and Monitoring

- Monitor transactions for consistency with the player's profile;
- Identify and investigate deviations or suspicious activity;
- Update player information as necessary.

5.4.3 PEP and Sanctions Screening

The Company must screen all players against international and local sanctions and PEP lists at onboarding and periodically thereafter.

Sanctions Screening:

- Players are checked against:
 - UN Sanctions List: <https://www.un.org/securitycouncil/content/un-sc-consolidated-list>
 - EU Sanctions Map: <https://www.sanctionsmap.eu>
 - Any local list issued by Curaçao authorities

PEP Screening:

- Sources include:
 - Publicly available news sources
 - The Transparency International Corruption Perceptions Index
 - www.knowyourcountry.com
 - PEP Caribbean List
- Where a customer is identified as a **PEP**, EDD is applied, including:
 - Senior management approval;
 - Identification of the source of wealth/funds;
 - Continuous enhanced monitoring.

5.4.4 Freezing of Funds and Reporting

If a player is identified as:

- A **designated person** under applicable sanctions;
- A **PEP** acting suspiciously;
- A **high-risk individual** linked to money laundering or terrorism;

Then the Company must:

1. **Immediately freeze the player's account** and block further transactions;
2. **File an Unusual Transaction Report (UTR)** with the **Financial Intelligence Unit (FIU) Curaçao**;
3. Avoid any action that could constitute **tipping-off** the player;
4. **Document the reasoning and actions taken** for compliance and audit purposes.

If the FIU determines the transaction is suspicious, it may refer the case for criminal investigation. The Company must **not disclose to the player** that a report has been made.

5.4.5 Tipping-Off Risk

The Company will continuously train its staff to avoid alerting a player when CDD, monitoring, or reporting actions are underway. Where performing CDD may increase the risk of tipping-off, the Company may defer the process and report directly to the FIU.

5.4.6 Documentation and Record-Keeping

All CDD information, risk assessments, verification data, and screening results must be:

- Retained for at least **five (5) years** after the end of the business relationship;
- Readily retrievable for inspection by competent authorities;
- Protected with strict confidentiality and access controls.

5.5 Ongoing Monitoring

Ongoing Monitoring of Customer Identity

The Company should conduct ongoing due diligence on the business relationship and maintain accurate, up-to-date identification data of its customers. Since customer identity details may change over time, the Company is encouraged to implement measures to detect and re-verify any changes in identification information. This may include periodically obtaining evidence of identity, refreshing identification data upon key events (such as changes in payment instruments), and tracking expiry dates of identity documents to ensure timely updates.

The Company ought to assess, on a risk-sensitive basis, whether any changes in customer information are substantial enough to require a re-assessment of the customer's risk profile within the business relationship.

Ongoing Monitoring of Transactions

The Company will take all possible efforts to perform continuous scrutiny of customer transactions to help prevent involvement in money laundering (ML) and terrorist financing (TF), and to protect its reputation. When transactions appear inconsistent with what the Company knows or expects from the customer, it is advisable to investigate such unusual activity.

If deviations from the customer's known source of funds, average profile, or account activity are detected, the Company is encouraged to understand the reasons behind these deviations and obtain sufficient information and documentation related to the transactions. Such situations may lead to revising the customer's risk profile.

After gathering the necessary information, the Company should consider whether the transaction is unusual and whether it needs to be reported to the Financial Intelligence Unit (FIU).

The level of ongoing monitoring is expected to be proportionate to the customer's risk profile. Even in low-risk cases, the Company is advised to maintain a degree of oversight to ensure that the business relationship continues to be classified as low risk.

This approach helps ensure that the Company's AML/CTF controls remain robust, risk-sensitive, and aligned with regulatory expectations for online gambling operations.

5.6 Reliance on Third Parties to Perform Customer Due Diligence

The Company may rely on third parties to perform certain elements of CDD, specifically elements a-c of the CDD measures, provided that specific criteria are met to ensure compliance and effectiveness.

Conditions for Reliance on Third Parties

1. Immediate Access to CDD Information

The Company should obtain the necessary information concerning elements a-c of the CDD measures immediately from the third party it relies upon.

2. Formal Agreement and Documentation Access

The Company is encouraged to have a formal agreement with the third party, stipulating that copies of identification data and other relevant documentation related to CDD requirements will be made available upon request. This arrangement should be periodically tested to ensure it functions as intended. Despite reliance on the third party, the Company retains ultimate responsibility for

conducting customer-based risk assessments, determining whether a customer is a Politically Exposed Person (PEP), and performing ongoing monitoring.

3. Verification of Third Party's Compliance and Regulation

The Company should satisfy itself that the third party is regulated, supervised, or monitored for compliance with CDD and record-keeping requirements consistent with applicable regulations. The third party must have an existing, independent business relationship with the customer and apply its own procedures to perform CDD measures.

4. Consideration of Country Risk

When determining the countries where the third party may be based, the Company should consider available information on the level of country risk to ensure appropriate risk management.

Distinction from Outsourcing or Agency Arrangements

Reliance on third parties for CDD differs from outsourcing or agency scenarios where the third party performs CDD on behalf of the Company according to the Company's procedures. In outsourcing arrangements, the Company remains responsible for the effective implementation and compliance of those procedures and should conduct periodic assessments of the service provider's performance both quantitatively and qualitatively.

Importantly, the decision to onboard a customer or to continue a business relationship based on risk assessment cannot be delegated or outsourced.

Responsibility for Agents and Group Companies

Any activities performed by agents or group companies are considered activities of the Company. Therefore, customers onboarded by agents or group companies must undergo the same checks and controls as those onboarded directly by the Company. It is the Company's responsibility to ensure that its AML/CTF controls, policies, measures, and procedures are fully applied by these entities.

This framework ensures that reliance on third parties for CDD is conducted within a controlled, compliant, and risk-sensitive environment, maintaining the integrity of the Company's AML/CTF program in the online gambling sector.

5.7 Reporting of unusual transactions

The Company should have clear procedures in place to recognize unusual transactions. Understanding the customer well is essential to identify transactions or series of transactions that deviate from the expected behavior based on the customer profile. Collecting and maintaining accurate customer information helps build this profile and assess associated risks.

Staff must receive specific guidance and training on recognizing and documenting unusual transactions, based on objective and subjective indicators established by applicable regulations. All unusual transactions should be reported internally to the Compliance Officer using the format approved by management. Supporting documents such as identification copies, transaction slips, and other relevant records must accompany the report. The Compliance Officer is responsible for maintaining an adequate filing system of these records.

If any internally reported transactions are not forwarded to the Financial Intelligence Unit (FIU), the reasons must be documented and signed off by the Compliance Officer and/or management.

Special attention should be given to complex, unusually large, or otherwise suspicious transaction patterns that lack an apparent economic or lawful purpose.

Examples of Unusual Transactions

Unusual transactions include, but are not limited to:

- Transactions linked to money laundering or terrorist financing investigations by law enforcement or justice authorities.
- Transactions involving persons or entities listed under applicable sanctions regulations.
- Transactions equal to or exceeding NAf. 5,000, including cash, checks, electronic payments, or other forms. Examples include:

- Cashless transfers from the Company's bank account to local or international accounts at the customer's request.
- Deposits or withdrawals of NAf. 5,000 or more.
- Purchase of gaming credits or tokens ("chips") amounting to NAf. 5,000 or more.
- Cash-outs of NAf. 5,000 or more.
- Transactions presumed to be related to money laundering or terrorist financing.

Note: A series or pattern of transactions within a single gaming day that cumulatively reach NAf. 5,000 or more are also considered unusual.

Reporting of Unusual Transactions

In accordance with applicable laws, the Company should report unusual or intended unusual transactions to the Curacao FIU without delay. Procedures for both internal and external reporting must be clearly established and communicated to all relevant personnel.

All unusual transactions must be reported internally immediately, with all supporting documentation submitted alongside the report.

The Compliance Officer is responsible for preparing and submitting reports to the FIU via the official goAML reporting portal. The Company must register with the FIU and obtain access credentials. Bulk reporting options may be available and should be discussed with the FIU account manager.

Reports and supporting documents should be submitted in English.

Confidentiality and Prohibition of Disclosure

The Company and its employees/contractors must not disclose any information related to reports filed with the FIU or requests made by the FIU. Disclosure to customers or third parties is strictly prohibited to avoid jeopardizing investigations.

The Company should exercise caution before terminating customer relationships or blocking transactions following a report. Drastic actions should be a last resort, as they may alert the customer and hinder ongoing investigations. Instead, enhanced monitoring and additional reporting are recommended when suspicious activity continues.

Record Keeping

The Company should retain all records related to transactions and customer due diligence for at least five years after the end of the business relationship or the date of an occasional transaction.

Records must be sufficient to reconstruct individual transactions, including amounts and currency types, to support potential criminal prosecutions.

All CDD documentation, such as copies of identification documents, account files, and business correspondence, must also be retained for the same period.

These records should be readily available to competent authorities upon lawful request.

This policy ensures the Company complies with its obligations to detect, document, and report unusual transactions effectively, thereby supporting the fight against money laundering and terrorist financing in the online gambling sector.

5.8 AML Compliance program

The Company maintains written AML policies and procedures, including a clear policy statement expressing its commitment to combat money laundering, terrorist financing, and proliferation financing. These policies reference relevant Curacao legislation (e.g., NOIS, NORUT, Sanctions National Ordinance) and set the organizational tone.

Detailed operating procedures translate policies into practical actions. The Company continuously monitors regulatory changes to keep the AML program current. Internal controls enable the Compliance Officer to detect deviations from established protocols.

All policies and procedures shall be approved by senior management and communicated to all employees/contractors.

5.8.1 Appointment of a Compliance Officer

A Compliance Officer, independent from operational functions, is formally appointed to oversee AML efforts. This officer has timely access to customer identification data, transaction records, and other relevant information and must act independently. The officer shall act independently and will be assigned at least the following responsibilities:

- Design and implement the Company's AML/CTF compliance program.
- Monitor adherence to local and international laws and regulations concerning AML/CTF.
- Review and ensure compliance with internal policies and procedures.
- Organize and deliver training sessions on compliance-related topics.
- Analyze and assess financial transactions for indicators of unusual or suspicious activity.
- Review internally reported unusual transactions and verify their accuracy and completeness.
- Maintain comprehensive records of all internal and external reports of unusual transactions.
- Establish internal procedures that define when and how unusual transaction reporting leads to account freezing or other mitigation actions, minimizing the risk of tipping off the player.
- Conduct deeper investigations into suspicious activities where warranted.
- Prepare and file external reports to the Financial Intelligence Unit (FIU) as required by NORUT.
- Recommend updates to the AML/CTF program as regulatory or risk conditions evolve.
- Stay current with local and international developments in AML/CTF and advise senior management accordingly.

The Compliance Officer's job description includes these duties and is formally acknowledged.

5.8.2 Employee Screening and Training Program

The Company commits to high ethical standards and compliance with financial laws through rigorous employee/contractors screening, including criminal background checks.

A comprehensive training program is provided to all employees/ contractors who handle customer transactions or AML-related duties. Training is tailored by role:

New employees/ contractors: General AML/CTF awareness, internal policies, and reporting obligations.

Frontline staff (dealers, cashiers): Specific training on recognizing and responding to money laundering risks in gambling operations.

Audit staff: Updates on regulatory changes and AML enforcement.

AML Compliance staff: Advanced training on emerging risks and regulatory expectations.

Supervisors and managers: In-depth instruction on AML policies and oversight responsibilities.

Senior management and board: Regular briefings on AML risks and reputational impacts.

Refresher training is conducted regularly, and detailed records of all training activities, participants, content, and outcomes are maintained.

6 Compliance and Consequences of Non-Compliance

6.1.Risks of Violating the Policy

Failure to comply with the Company's AML/CTF policy exposes the organization to significant risks, including:

- **Legal and Regulatory Risks:** Non-compliance may result in violations of Curacao laws and international regulations, leading to fines, sanctions, or revocation of licenses.
- **Reputational Risks:** Breaches can damage the Company's reputation, undermining customer trust and business relationships.

- **Financial Risks:** The Company may face substantial financial penalties, increased scrutiny, and potential loss of business opportunities.
- **Operational Risks:** Non-compliance can disrupt business operations, including forced suspension of services or regulatory investigations.

6.2. Potential Consequences for Individuals

Employees or agents who violate the policy may face:

- **Disciplinary Actions:** These can range from warnings and retraining to suspension or termination of employment, depending on the severity of the breach.
- **Legal Implications:** Individuals may be subject to civil or criminal liability, including fines or prosecution, if involved in or negligent towards money laundering or terrorist financing activities.

6.3. Business Consequences

The Company may suffer:

- Loss of operating licenses or regulatory approvals.
- Increased regulatory oversight and audit frequency.
- Damage to partnerships and customer confidence.
- Financial losses due to penalties and remediation costs.

7.Commitment to Compliance

The Company is committed to enforcing this policy strictly and expects all employees, contractors, and partners to adhere fully. Prompt reporting of any suspected breaches or suspicious activities is mandatory to mitigate risks and ensure regulatory compliance.

8. Policy History

This is a revised 3.0 Version of AML policy established to formalize the Company's AML and CTF framework in compliance with recent Curacao regulations.

Version	Effective Date	Description of Changes
1.0	April 27, 2023	Initial AML policy
2.0	July 19, 2024	Amended AML Policy
3.0	July 20, 2025	Revised AML Policy