

GAMEPLAY INTERNATIONAL B.V.

Reg. Number: 148409

Dr. H. Fergusonweg 1, Willemstad, Curaçao

AML/CTF/CPF POLICY

Version 3

Approved by the Board of Directors



(SMES)

**Solutions for Management
and Employment Support N.V.**

Responsible Compliance Officer:

Semen Klyuchyk

compliance@gameplayinternational.com

Version 1: 20-02-2025

Version 2: 28-03-2025

Version 3: 15-12-2025

Next Review: December, 2026

TABLE OF CONTENTS

1. Statement	2
2. Abbreviations & Definitions	3
3. iGaming Environment	6
4. Money Laundering, Terrorism Financing& Proliferation Financing	7
5. Integration of the Risk Assessment & Ongoing Monitoring	13
6. Risk-Based Approach	20
7. Customer Due Diligence & Enhanced Due Diligence	24
8. Customer Acceptance Policy	28
9. Transaction Monitoring	46
10. Politically Exposed Persons	48
11. Sanctions Policy	50
12. Suspicious & Unusual Activity & Transaction Reporting	54
13. Compliance Officer	59
14. Senior Management	61
15. Employee Training & Screening	62
16. AML Compliance Audit	64
17. Regulatory Access & Cooperation	66
18. Internal Audit & Reporting	68
19. Record-Keeping	70
20. Appendices	71
Appendix 1: Customer Risk Calculator	71
Appendix 2: Employee Onboarding & Screening Form	72

1. Statement

This Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Policy (hereinafter, the “Policy”) applies to GAMEPLAY INTERNATIONAL B.V., a company incorporated under the laws of Curaçao (hereinafter, the “Company”).

GAMEPLAY INTERNATIONAL B.V. is dedicated to the prevention of financial crimes, including money laundering, terrorism financing, and proliferation financing. To achieve this, the company has instituted a comprehensive Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Policy (AML/CTF/CPF Policy), which ensures compliance with both national and international regulatory frameworks. This policy serves as a structured risk management approach covering essential operational areas such as customer interactions, product and service offerings, payment channels, geographic locations, and service delivery methods, aligning with the highest regulatory standards and ensuring strict adherence to all relevant legal obligations.

The Board of Directors (BoD) of GAMEPLAY INTERNATIONAL B.V. is responsible for the approval, enforcement, and oversight of this AML/CTF/CPF Policy. To maintain its effectiveness, the policy undergoes an annual review, with amendments introduced as necessary to reflect regulatory updates or operational adjustments. Additionally, a designated compliance officer is authorized to recommend immediate updates to the policy based on findings from internal or external AML audits, ensuring that any potential risks are promptly mitigated.

GAMEPLAY INTERNATIONAL B.V. strictly follows key international and Curaçao regulatory mandates concerning anti-money laundering, counter-terrorism financing, and counter-proliferation financing. Compliance with these regulations is an essential requirement for maintaining an iGaming license under the Curaçao jurisdiction. The legal framework governing these obligations includes:

- The National Ordinance on Identification When Rendering Services (NOIS) (N.G. 2017, no. 92) - Article 2(8) and Article 11(3)
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99) - Article 22mm(3)
- Sanctions National Ordinance (N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)

The Curaçao Gaming Control Board (GCB) provides a structured compliance framework guiding casinos and online gambling operators in adhering to these regulations. This framework serves as the foundation for GAMEPLAY INTERNATIONAL B.V.'s internal policies and procedures aimed at reducing financial crime risks.

GAMEPLAY INTERNATIONAL B.V. complies with various regulatory provisions, including but not limited to:

- National Ordinance on Identification of Clients When Rendering Services (N.G. 2017, no. 92)
- National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99)
- Ministerial Decree (November 11, 2015) - 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 on the Enforcement of the Kingdom Sanction Law (N.G. 2017, no. 2)
- National Decree (July 10, 2015) - Implementation of UN Security Council Resolutions (N.G. 2015, no. 29)
- National Decree (July 10, 2015) - Sanctions Ordinance Libya (N.G. 2015, no. 28)
- National Decree (July 10, 2015) - Extension of Validity Sanction Decrees 2018 (N.G. 2018, no. 34)
- The Penal Code (Code of Criminal Law) (N.G. 2011, no. 48)

These laws, in conjunction with regulations stemming from NOIS, NORUT, the Sanctions National Ordinance, and the Kingdom Sanction Law, form the core legal framework governing the Curaçao gaming sector's AML/CTF/CPF responsibilities.

Beyond compliance with local regulations, this policy integrates global best practices and follows guidelines established by key international organizations, including:

- Financial Action Task Force (FATF) Recommendations
- European Union's 4th, 5th, and 6th Anti-Money Laundering Directives (AMLDs)
- The Wolfsberg Principles

By incorporating these international frameworks, GAMEPLAY INTERNATIONAL B.V. reinforces its commitment to preventing financial crimes and ensuring its regulatory approach aligns with global standards.

The AML/CTF/CPF Policy of GAMEPLAY INTERNATIONAL B.V. is designed to meet the compliance requirements set by the Curaçao Gaming Control Board. All directors, officers, employees, and third-party compliance auditors are required to fully comply with and uphold the principles outlined in this policy. Through strict enforcement and continuous monitoring, GAMEPLAY INTERNATIONAL B.V. remains dedicated to fostering a secure and legally compliant gaming environment while preventing illicit financial activities within its operations.

2. Abbreviations & Definitions

AML (Anti-Money Laundering) – A set of laws, regulations, and procedures designed to prevent money laundering and other financial crimes.

CTF (Counter-Terrorism Financing) – The process of identifying and preventing

financial transactions that support terrorist activities.

CPF (Counter-Proliferation Financing) – Measures aimed at stopping financial support for the spread of weapons of mass destruction.

KYC (Know Your Customer) – Procedures used to verify the identity of customers and monitor their financial activities.

CDD (Customer Due Diligence) – A process of verifying customer identity, assessing risk, and monitoring transactions to detect potential illicit activity.

EDD (Enhanced Due Diligence) – Additional verification and risk assessment measures applied to high-risk individuals, businesses, or transactions.

UBO (Ultimate Beneficial Owner) – The individual who ultimately owns or controls an account or financial transaction.

SOF/SOW (Source of Funds/Source of Wealth) – Verification of the origin of financial assets to ensure they are not derived from criminal activities.

PEP (Politically Exposed Person) – An individual holding a high-profile political or public function who requires additional scrutiny due to increased financial crime risks.

SAR/STR (Suspicious Activity Report/Suspicious Transaction Report) – A report submitted to regulatory authorities when a transaction or financial activity appears suspicious or unusual.

FIU (Financial Intelligence Unit of Curaçao) – The national agency responsible for analyzing and processing reports on suspicious financial transactions.

BoD (Board of Directors) – The company's governing body responsible for compliance oversight, corporate governance, and regulatory adherence.

Compliance Officer – A senior official responsible for managing AML/CTF/CPF risks, ensuring compliance with financial crime regulations, and operating independently from gaming operations.

NOOGH (National Ordinance on Offshore Games of Hazard) – Curaçao's legislative framework governing offshore gaming activities.

OFAC (Office of Foreign Assets Control) – A U.S. Treasury Department agency that enforces economic sanctions against targeted individuals, entities, and countries.

FATF (Financial Action Task Force) – An international organization that develops and promotes global AML and CTF standards and monitors high-risk jurisdictions.

CFATF (Caribbean Financial Action Task Force) – A regional group of Caribbean, Central, and South American countries dedicated to combating money laundering and terrorist financing.

EU (European Union) – A political and economic union that enforces AML/CTF directives among its member states.

UK (United Kingdom) – A jurisdiction with AML/CTF regulations overseen by its financial and regulatory authorities.

US (United States) – A country with financial crime oversight conducted by agencies such as OFAC and FinCEN.

Risk-Based Approach (RBA) – A methodology for assessing and managing AML/CTF risks based on transaction types, customer profiles, and jurisdictions.

Blacklist – A list of individuals, businesses, or jurisdictions subject to financial restrictions due to regulatory concerns.

Sanctions – Legal restrictions imposed on specific countries, individuals, or entities due

to financial crime, national security risks, or geopolitical concerns.

Automated Screening Tools (AST) – Software that screens customers against sanctions lists and flags high-risk individuals or transactions.

Economic Sanctions – Financial and trade restrictions imposed by governments or regulatory bodies to restrict illicit financial activity.

Curaçao Gaming Control Board (GCB) – The primary supervisory authority responsible for overseeing AML/CTF compliance in the gaming sector.

Know Your Business (KYB) – The process of verifying business entities, their ownership structures, and financial activities for compliance purposes.

Structuring – A money laundering technique that involves breaking large transactions into smaller amounts to evade reporting thresholds.

Layering – A method used to disguise the source of illicit funds by conducting multiple, complex transactions.

Integration – The final stage of money laundering, in which illicit funds are reintroduced into the legitimate economy.

Sanctions Evasion – Attempts to circumvent restrictions by disguising transactions involving sanctioned individuals, entities, or countries.

Financial Action Task Force (FATF) – A global authority that sets AML/CTF compliance standards and issues blacklists and greylists for high-risk countries.

First Line of Defense – Employees responsible for collecting customer information and identifying suspicious activity during onboarding and transaction processing.

Suspicious Transaction Report (STR) – A report submitted to regulatory authorities when a transaction raises AML/CTF concerns.

Egmont Group of FIUs – An international network of Financial Intelligence Units that facilitates cooperation and intelligence-sharing in financial crime investigations.

The Wolfsberg Group – An association of major global banks that develops best practices for private banking AML compliance.

Money Laundering Reporting Officer (MLRO) – The designated officer responsible for overseeing AML policies, conducting transaction monitoring, and submitting SARs/STRs.

Audit Logs – Records maintained for compliance and regulatory review, documenting AML/CTF efforts and stored for a minimum of five years.

Reporting Mechanism Audit – A process that ensures SARs and other compliance reports meet legal standards and are properly documented.

Unusual Transaction – A financial activity that deviates from normal transaction patterns and may indicate illicit activity.

Transaction Monitoring – The real-time analysis of financial transactions to identify suspicious behavior and detect money laundering risks.

High-Risk Third Country – A jurisdiction identified by FATF or the European Commission as having insufficient AML/CTF controls.

Comprehensive Sanctions – The strictest level of sanctions, prohibiting all financial dealings with a sanctioned country, individual, or entity.

Sanctions Compliance and Screening – The process of verifying customers and transactions against international sanctions lists to prevent illicit financial activity.

Operational Restrictions – Limitations imposed on businesses that fail to comply with

AML/CTF regulations, including license suspensions and financial penalties.

Risk Appetite – The level of risk an organization is willing to accept within its AML/CTF compliance framework.

Beneficial Owner – The individual who ultimately controls or benefits from a financial transaction or legal entity.

Financial Crime Prevention Framework – A structured program designed to mitigate money laundering, terrorist financing, and other financial crimes.

Customer File Review – A compliance practice where customer records are periodically examined to ensure adherence to KYC, CDD, and regulatory requirements.

Senior Management Oversight – The responsibility of executive leadership to ensure that AML/CTF/CPF programs are effectively implemented and continuously improved.

Training and Awareness Programs – Educational initiatives designed to ensure employees understand AML/CTF risks, compliance obligations, and reporting procedures.

Ongoing Monitoring – A continuous review of customer transactions and risk profiles to identify potential financial crime risks.

Regulatory Reviews – Assessments conducted by supervisory authorities to verify that a company's AML/CTF policies and practices meet legal requirements.

Corrective Action Plans – Compliance strategies implemented in response to audit findings or regulatory enforcement actions.

Periodic Independent Audits – External reviews of a company's AML/CTF/CPF compliance framework to identify gaps and improve regulatory adherence.

Internal Control Mechanisms – Policies and procedures designed to safeguard against financial crime risks and ensure compliance with AML regulations.

Real-Time Risk Assessment – The use of technology and compliance teams to assess and respond to potential money laundering threats as transactions occur.

Confidentiality in Reporting – The requirement to protect information related to SARs/STRs, preventing unauthorized disclosure or tipping off of customers.

3. iGaming Landscape

GAMEPLAY INTERNATIONAL B.V. (hereinafter, the “Company”) is a legally registered entity in Curaçao that operates the website <https://bizbet.io/en>. The company holds an online gaming license issued by the Curaçao Gaming Control Board (OGL/2024/511/0630), ensuring full compliance with licensing regulations and regional restrictions set by Curaçao regulatory authorities. These regulations strictly prohibit remote gaming licensees from offering services in specific jurisdictions, including the United States, Australia, the Dutch West Indies (Aruba, Bonaire), Curaçao, France, Germany, the United Kingdom, Belize, and the Netherlands. As a result, GAMEPLAY INTERNATIONAL B.V. operates exclusively in legally authorized markets and does not target customers in regions where online gambling is restricted or prohibited.

As with other e-gaming and betting operators, GAMEPLAY INTERNATIONAL B.V. faces potential money laundering risks, such as identity theft, fraudulent activities, structuring, layering, and the possibility of collusion among employees, customers, or third-party payment providers seeking to circumvent internal security measures. To mitigate these risks, the company has established a robust AML/CTF/CPF framework, implementing strict security protocols and due diligence measures to prevent illicit financial activities within its operations.

4. Money Laundering, Terrorism Financing & Proliferation Financing

Money Laundering:

Money laundering plays a critical role in financial crimes, often involving international transactions and operations. It is associated with a range of illegal activities, including tax fraud, corruption, sanctions evasion, drug trafficking, illicit arms trade, extortion, and kidnapping. The primary purpose of money laundering is to obscure the illegal origins of financial gains, making it difficult to trace their source, ownership, and ultimate destination.

The Three Stages of Money Laundering

1. **Placement** – This initial phase involves introducing illegally obtained funds into the financial system. This can occur through bank deposits, acquiring high-value assets, or conducting various financial transactions. The objective at this stage is to begin integrating illicit proceeds into the legitimate economy.
2. **Layering** – During this stage, funds are transferred through multiple transactions to create complexity and obscure their origins. This may involve moving money between multiple accounts, converting funds into different currencies, or investing in financial instruments. The intent is to make tracing the transactions back to their criminal source increasingly difficult.
3. **Integration** – In the final phase, laundered funds are reintroduced into the legal economy. This may involve purchasing luxury assets, investing in cash-intensive businesses, or engaging in other seemingly lawful financial activities. At this stage, the illicit funds appear legitimate, making them harder to identify and track.

Money laundering can take place at various points within financial transactions, and online gambling platforms are particularly vulnerable to exploitation. This highlights the necessity of preventing anonymous transactions and promptly identifying suspicious activity.

Terrorist Financing and Its Link to Money Laundering

Terrorist financing refers to the movement of funds intended to support terrorist activities. Unlike traditional money laundering, these funds may come from lawful

sources but are processed in a manner that mirrors laundering techniques. For example, prepaid cards are often used to finance terrorist operations by purchasing supplies for attacks.

To mitigate such risks, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) ensures that employees receive continuous training on emerging trends and evolving threats associated with terrorist financing.

Risk Management and Compliance Measures

To proactively combat money laundering risks, GAMEPLAY INTERNATIONAL B.V. has implemented comprehensive compliance measures to identify, assess, and mitigate potential threats. These include:

- Fraud Prevention and Identity Verification – Conducting customer due diligence (CDD) through document verification, age authentication, and location validation.
- Monitoring Multiple Accounts and High-Value Transactions – Identifying irregular account behavior, such as the use of multiple accounts or frequent large transactions.
- Detecting Suspicious Deposits – Screening for funds that may originate from illicit activities and ensuring the platform is not misused as a temporary holding space for such transactions.
- Player-to-Player Transfers – Monitoring transactions between users to detect potential misuse for laundering illicit funds or fraudulent cash-outs.

These measures represent key components of the company's AML compliance efforts; however, new risks may emerge over time. To ensure continued effectiveness, GAMEPLAY INTERNATIONAL B.V. conducts regular risk assessments tailored to evolving threats and provides ongoing training to its employees. This reinforces the company's commitment to a robust Anti-Money Laundering (AML) compliance framework.

Terrorism Financing:

Terrorism financing involves the provision of financial support to terrorist organizations or activities, utilizing both lawful and unlawful financial sources. These funds are essential for carrying out operations, ranging from minor logistical support to large-scale attacks.

Sources of Terrorism Financing

The funding sources for terrorist activities can generally be categorized into two groups:

- Legitimate Sources – Terrorists often exploit legal financial systems, including businesses, charitable donations, and other lawful transactions, to redirect funds

covertly. In some instances, charitable organizations and commercial enterprises are misused as intermediaries to conceal and reroute financial resources.

- Illicit Sources – Criminal activities such as fraud, smuggling, drug trafficking, extortion, and money laundering serve as primary means of generating funds while obscuring their origins.

Methods of Fund Transfers

Terrorist networks employ various channels to transfer and distribute funds, including:

- Formal Financial Institutions – Traditional banking systems and financial services are sometimes manipulated using advanced techniques such as layering and structuring. These methods involve breaking large transactions into smaller amounts to avoid raising suspicion and bypass financial monitoring mechanisms.
- Informal Money Transfer Systems – Alternative financial networks, such as the hawala system, operate outside conventional banking regulations, making it difficult for authorities to detect and trace suspicious transactions.

Indicators of Terrorism Financing

Certain financial behaviors and transaction patterns may signal potential terrorist financing, including:

- Unusual financial activities that deviate from an individual's or business's normal behavior.
- Frequent or high-value transactions linked to regions associated with terrorist activity.
- Financial dealings involving individuals or organizations flagged on international sanctions or watchlists.
- Large cash deposits, transactions involving high-risk industries, or activities designed to evade detection by financial institutions.

Regulatory Compliance and Countermeasures

To mitigate the risks associated with terrorism financing, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) has established a robust Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) compliance framework, which includes:

- Customer Due Diligence (CDD) – Conducting thorough identity verification, assessing the source of funds, and evaluating potential risks.
- Transaction Monitoring – Continuously analyzing financial transactions to detect patterns indicative of suspicious activities.
- Reporting Suspicious Activities – Promptly notifying the relevant authorities whenever transactions raise red flags related to terrorism financing.

Furthermore, the company strictly adheres to various international and national regulatory frameworks, including:

- Sanctions National Ordinance (SNO, N.G. 2014, no. 55)
- Kingdom Sanction Act (N.G. 2016, no. 54)
- Curaçao Gaming Control Board (GCB) regulatory requirements
- Office of Foreign Assets Control (OFAC) sanctions and watchlists
- United Nations Security Council (UNSC) sanctions list
- European Union (EU) anti-terrorism financing regulations
- U.S. List of Foreign Terrorist Organizations

These regulatory measures ensure that GAMEPLAY INTERNATIONAL B.V. does not inadvertently facilitate financial transactions that could support terrorist organizations.

Global Counter-Terrorism Financing Initiatives

To align with international standards, GAMEPLAY INTERNATIONAL B.V. complies with established counter-terrorism financing frameworks, including:

- Financial Action Task Force (FATF) – An international body that sets guidelines for detecting and preventing financial crimes related to terrorism and money laundering.
- Office of Foreign Assets Control (OFAC) – A U.S. government agency responsible for enforcing economic sanctions and maintaining the Specially Designated Nationals (SDN) list, which includes entities linked to terrorism.
- European Union (EU) Regulations – Mandating strict AML/CTF measures across member states to prevent financial exploitation by terrorist groups.
- United Nations (UN) Sanctions – Imposing global restrictions and maintaining watchlists of individuals and organizations associated with terrorism financing.

By implementing stringent compliance policies and adhering to international regulations, GAMEPLAY INTERNATIONAL B.V. reinforces its ability to identify, prevent, and report terrorism financing activities, ensuring a secure and legally compliant operational environment.

Proliferation Financing:

Proliferation financing refers to the financial support, facilitation, or provision of resources for activities related to the development, acquisition, and distribution of weapons of mass destruction (WMDs) and their delivery systems. This form of financial crime poses a significant global security risk and is strictly prohibited under both international regulations and Curaçao's legal framework. As a licensed iGaming operator, GAMEPLAY INTERNATIONAL B.V. (Reg. Number: 148409) is committed to identifying, assessing, and mitigating the risks associated with proliferation financing. This commitment is embedded within the company's broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF)

compliance framework, ensuring full regulatory adherence and the integrity of its financial transactions.

Compliance with Curaçao iGaming Regulations

The Curaçao Gaming Control Board (GCB) enforces strict regulatory requirements to prevent financial crimes, including proliferation financing. These regulations require all licensed iGaming operators, including GAMEPLAY INTERNATIONAL B.V., to take active measures in identifying, mitigating, and reporting potential threats linked to WMD proliferation. By complying with these regulations, the company aligns itself with global financial security standards, ensuring that its platform is not exploited for illicit financial activities.

Risk Assessment and Proliferation Financing Prevention

To effectively counter the risks associated with proliferation financing, GAMEPLAY INTERNATIONAL B.V. conducts comprehensive risk assessments on an ongoing basis. These assessments focus on identifying customers and financial transactions that may be linked to high-risk jurisdictions known for weak proliferation controls. In particular, the company examines transactions involving goods, services, or entities associated with proliferation networks and evaluates financial patterns that resemble established proliferation financing methods. By continuously refining its risk assessment strategies, the company enhances its ability to detect and prevent any attempts to misuse its platform for illicit financial purposes.

Enhanced Customer Due Diligence (CDD) Measures

As part of its stringent compliance framework, GAMEPLAY INTERNATIONAL B.V. implements enhanced customer due diligence (CDD) procedures, particularly for customers and transactions categorized as high-risk. These procedures include screening all customers against international sanctions lists, including those maintained by the United Nations Security Council (UNSC), the Financial Action Task Force (FATF), and the European Union (EU). Additionally, the company thoroughly investigates any transactions that deviate from typical customer behavior and closely monitors potential affiliations with organizations flagged for involvement in proliferation-related activities. These proactive measures ensure that the company effectively identifies and prevents high-risk transactions from occurring within its platform.

Transaction Monitoring and Suspicious Activity Reporting

To detect financial activities that may be linked to proliferation financing, GAMEPLAY INTERNATIONAL B.V. employs sophisticated transaction monitoring systems designed to analyze patterns of financial behavior. These systems continuously scan financial transactions, flagging any movements that exhibit characteristics of proliferation financing. When suspicious activity is identified, it is immediately reviewed by compliance officers, who conduct further investigations before submitting Suspicious Activity Reports (SARs) to the Curaçao Financial Intelligence Unit (FIU). This ensures

that regulatory authorities are promptly informed of any potential proliferation financing risks, enabling swift enforcement actions against any entities attempting to exploit the financial system.

Sanctions Screening and Regulatory Compliance

Strict adherence to Curaçao and international sanctions regulations is a core component of GAMEPLAY INTERNATIONAL B.V.'s compliance program. The company systematically screens all financial transactions and business relationships against regularly updated sanctions lists, including those under the Kingdom Sanction Act and United Nations Security Council Resolutions. Transactions involving individuals, entities, or jurisdictions subject to WMD-related sanctions are automatically flagged and blocked, preventing illicit financial flows from infiltrating the platform. Additionally, the company maintains detailed records of all sanctions screenings and compliance actions, ensuring full transparency and accountability during regulatory audits.

Training and Awareness for Employees

Recognizing the importance of informed decision-making in preventing proliferation financing, GAMEPLAY INTERNATIONAL B.V. ensures that all employees receive specialized training on financial crime risks, with a particular focus on proliferation financing threats. This training enables employees to recognize key red flags, such as unusual financial transactions or suspicious business affiliations, and equips them with the knowledge required to respond appropriately to potential threats. Additionally, the company's training programs are regularly updated to reflect the latest developments in Curaçao's evolving regulatory landscape, ensuring that compliance personnel remain vigilant against emerging risks.

Collaboration with Regulatory Authorities

In its commitment to upholding financial integrity, GAMEPLAY INTERNATIONAL B.V. actively collaborates with regulatory bodies and enforcement agencies, including the Curaçao Gaming Control Board (GCB), the Financial Intelligence Unit (FIU), and other relevant authorities. This collaboration involves sharing intelligence on potential threats, providing timely reports on suspicious activities, and actively participating in industry-wide initiatives aimed at strengthening the iGaming sector's defenses against proliferation financing risks. By fostering strong regulatory partnerships, the company plays a vital role in preventing its platform from being misused for unlawful financial activities.

Commitment to Global Security and Compliance

As a responsible iGaming operator, GAMEPLAY INTERNATIONAL B.V. remains unwavering in its dedication to preventing proliferation financing activities within its platform. The company's adherence to Curaçao's latest iGaming regulations and international compliance frameworks ensures that it upholds the highest standards of financial security, transparency, and legal compliance. These efforts not only safeguard

the integrity of the company's financial operations but also contribute to global initiatives aimed at disrupting financial networks linked to WMD development and distribution. By maintaining rigorous compliance controls, the company strengthens its role as a trusted and responsible participant in the international financial system.

5. Integration of the Risk Assessment & Ongoing Monitoring

The Company maintains a structured and responsive compliance framework to address the risks associated with money laundering, terrorism financing, and the funding of weapons of mass destruction. This framework is designed to protect its operations in online gaming, financial transactions, and digital platforms. It is implemented in full accordance with the applicable laws and regulations of Curaçao, including the obligations imposed by the Curaçao Gaming Control Board (GCB), and follows international standards set by the Financial Action Task Force (FATF) and the Caribbean FATF (CFATF). All parties involved with the Company, such as employees, executives, third-party providers, and business partners, are expected to observe these standards.

Governance and Oversight

The Board of Directors holds overall responsibility for ensuring that the Company's AML, CTF, and CPF compliance program is properly implemented. It is responsible for allocating the necessary resources to manage industry-specific risks effectively. Senior Management is responsible for executing these strategic directives and ensuring that the Compliance Officer has full and unhindered access to the data, systems, tools, and personnel required to fulfil their obligations.

Role of the Compliance Officer and Use of the NRA

The Compliance Officer is responsible for day-to-day compliance management. This includes oversight of customer due diligence procedures, transaction monitoring, internal investigations, and the submission of reports to the Financial Intelligence Unit (FIU) of Curaçao. In accordance with AML Regulation III.1, the Compliance Officer ensures that internal controls are regularly reviewed and updated to reflect evolving regulatory standards and financial crime risks.

The Company also applies the findings of the most recent National Risk Assessment (NRA) conducted by Curaçao's authorities. These findings are used across different areas of operations to re-evaluate customer risk profiles, assess exposure to different countries, review the use of financial technologies, and refine internal controls in line with emerging risks and threat typologies.

Operational Implementation of NRA Findings

Insights from the NRA are incorporated into the Company's broader institutional risk framework. The Compliance Officer takes specific action based on these findings, including:

- Strengthening identity verification and onboarding procedures
- Adjusting transaction monitoring parameters to reflect new risk patterns
- Implementing additional controls for customers, jurisdictions, or payment methods identified as high risk
- Deploying advanced monitoring tools tailored to newly identified threat indicators

When new risks emerge, the Compliance Officer evaluates whether existing controls are sufficient and enhances them as necessary.

Risk-Based Due Diligence

The Company applies risk-based Know Your Customer (KYC) procedures, especially before processing withdrawals or when transaction activity exceeds defined limits. Basic due diligence involves verification of identity, address, age, and payment method. If risk factors are present, particularly those highlighted in the NRA, Enhanced Due Diligence (EDD) is required. EDD may include:

- Collection of documents proving source of funds and wealth
- Expanded checks using open-source and regulatory information
- Escalation for approval by senior compliance or management staff

EDD is mandatory for high-risk groups, including politically exposed persons (PEPs), users from high-risk countries, customers with large transaction volumes, or those displaying unusual behaviour.

Monitoring and Escalation

A dual-layer monitoring system is in place, combining automated checks with manual review. The system is designed to detect:

- Irregular deposit and withdrawal patterns
- Unusual betting activity
- Use of proxy or VPN services to disguise location

- Repeated changes to account information or misuse of bonuses

Alerts generated by the system are escalated to the Compliance Officer for investigation. If a transaction is deemed suspicious, it is reported to the FIU through the goAML platform in compliance with AML Regulation IV.1 and the National Ordinance on the Reporting of Unusual Transactions (NORUT).

All staff are required to escalate suspicious behaviour without delay. Disclosure of such investigations to the subject or other parties is strictly prohibited. Any breach is treated as a serious disciplinary matter.

Recordkeeping and Training

The Company stores all compliance-related documentation for a minimum period of five years. This includes customer verification records, transaction histories, alerts, internal reviews, and audit results, as well as materials relating to the NRA.

Employees involved in compliance duties receive regular training that includes specific modules on the NRA and national-level risks. Training is conducted annually and updated as needed to reflect new laws or threats. The Compliance Officer ensures that all policies are reviewed at least once per year and updated to incorporate NRA findings and guidance issued by the GCB.

Customer Risk Assessment

The Company applies a systematic, risk-based model to evaluate each customer's exposure to potential money laundering, terrorist financing, and proliferation financing. This approach is anchored in a structured risk scoring framework that takes into account the customer's behavior, geographic exposure, and other key indicators. The aim is to ensure that the level of due diligence and ongoing monitoring corresponds appropriately to the customer's risk level.

Risk Scoring Methodology

Each identified risk factor is assigned a numeric value. The total score determines the customer's classification, which in turn dictates the applicable due diligence measures and the internal approval level required at onboarding and during the ongoing relationship.

Risk Category	Score Range	Due Diligence Level	Approval Required
Low Risk	0 to 1.8	Standard Due Diligence	Client Services or Compliance Officer
Medium Risk	1.8 to 2.5	Standard Due Diligence	Client Services or Compliance Officer
High Risk	2.5 or higher	Enhanced Due Diligence	Compliance Officer, reviewed annually
Unacceptable Risk	Trigger-based	Rejected	Automatically declined

Customers in the low or medium risk categories are subject to standard due diligence procedures. These include verification of identity, periodic review of customer data, and transaction analysis. High-risk clients are subject to enhanced due diligence, which includes submission of supporting documentation, mandatory review by the Compliance Officer, and annual reassessment.

If a customer is determined to present an unacceptable risk, such as being subject to sanctions or exhibiting severe red flags, their application is declined. No relationship is established under such circumstances.

The Company regularly updates its risk assessment methodology in line with evolving regulatory standards, emerging criminal typologies, and industry-wide developments.

Screening and Risk Management

All customers undergo screening at the time of onboarding and on an ongoing basis. This includes checks for:

- Sanctions exposure at the domestic and international levels
- Status as a Politically Exposed Person (PEP)
- Negative information in media or regulatory reports

These checks are applied regardless of the customer's risk category.

Low-Risk Customers

Customers classified as low risk are not automatically eligible for simplified due diligence due to the inherent risk associated with online gaming operations. Standard due diligence still applies in full, in accordance with internal policy and Curaçao's regulatory framework.

Medium-Risk Customers

Medium-risk clients present moderate risk indicators. These customers are required to satisfy all KYC requirements and are reviewed periodically to verify the accuracy of their risk classification.

High-Risk Customers

Customers in this category are subject to the highest level of scrutiny. Approval by the Compliance Officer is required before account activation or continuation of the business relationship. High-risk indicators may include:

- Use of complex corporate structures or opaque ownership
- Transactions that do not match expected financial behavior
- Connections to high-risk or sanctioned jurisdictions
- Identification as a PEP or association with a PEP
- Adverse media reports or regulatory sanctions
- Provision of falsified or unverifiable documents
- Transactions without a clear legal or economic purpose
- Acting on behalf of another person or facilitating third-party payments
- Cumulative deposits surpassing high-risk thresholds

Unacceptable Risk Profiles

The Company does not accept customers who:

- Appear on any relevant sanctions list
- Are suspected of involvement in money laundering, terrorism financing, or proliferation financing
- Are under 18 years of age or fail age verification

- Cannot demonstrate the origin of their funds or source of wealth
- Exhibit abusive or manipulative behavior within the gaming platform

The Company maintains a clearly defined risk appetite. Customers whose profiles exceed this threshold are rejected without exception. All decisions, whether related to onboarding, escalation, or rejection, are fully documented and stored for compliance and audit purposes.

The customer risk assessment framework is subject to ongoing enhancement based on internal reviews and regulatory or typological updates.

Ongoing Monitoring

The Company implements a continuous customer monitoring program as part of its risk-based compliance framework. This program ensures that customer data remains accurate and up to date, while enabling the detection and escalation of any unusual or suspicious activities. All procedures are carried out in alignment with Curaçao's Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing requirements.

Continuous Screening Procedures

The Compliance Department performs regular screening of active customer accounts using external data sources. These include international sanctions lists, databases of Politically Exposed Persons (PEPs), and adverse media platforms. When a confirmed match is identified, the case is escalated to compliance personnel for review. If needed, this may result in an immediate reassessment of the customer's risk rating.

Event-Driven Reviews

The Company conducts targeted reassessments of customer profiles in response to specific events or identified risks. Such reviews may involve updating due diligence documentation and revising the customer's risk classification. Triggers for an event-based reassessment include:

- Receipt of new information that contradicts or invalidates previously verified customer details
- Transactions or patterns that significantly deviate from expected behavior
- Identification of new risk factors that affect the customer's risk profile

Upon initiating such a review, the customer's classification is promptly re-evaluated, and all related internal records are updated without delay.

Periodic Risk-Based Reviews

In addition to event-driven assessments, the Company performs scheduled reviews based on the customer's risk level:

- High-risk customers are reviewed once per year. This includes reconfirming residential address, verifying source of funds and wealth, performing updated adverse media screening, and reviewing account activity.
- Medium-risk customers undergo profile reviews every two years. These reviews focus on updating customer information, validating financial and behavioral patterns, and ensuring ongoing compliance.
- Low-risk customers are reviewed every three years. These reviews involve reconfirming identification documents and checking for any new adverse information that may impact the low-risk status.

The Company may initiate unscheduled reviews at any time if:

- New risk indicators are detected
- Suspicious or abnormal behavior is observed
- Regulatory updates or changes in the sector risk profile require re-evaluation

Integration of National Risk Assessment (NRA)

The Company adjusts its monitoring framework in response to the latest National Risk Assessment issued by authorities in Curaçao. When the NRA identifies new typologies or shifts in threat levels, the Compliance Officer updates internal processes accordingly. This may include:

- Modifying transaction monitoring parameters
- Updating control mechanisms and alert triggers
- Revising the customer risk evaluation methodology to reflect revised typologies

Commitment to a Responsive Compliance Framework

By integrating domestic and global risk trends into its monitoring procedures, the Company maintains a proactive approach to financial crime prevention. This adaptive monitoring strategy enables timely detection of threats and supports full regulatory

compliance, helping to protect the integrity of the platform from misuse or exposure to illicit activity.

6. Risk-Based Approach

The Company applies a comprehensive and structured risk-based methodology to detect, assess, and manage the risk of its online gaming platform being misused for money laundering, terrorist financing, or the financing of weapons proliferation. This strategy is consistent with the principles set out by the Financial Action Task Force (FATF) and integrates both qualitative and quantitative assessments of threats, vulnerabilities, mitigation strategies, and potential business impact.

A detailed Business Risk Assessment (BRA) is conducted annually and whenever there are significant changes to products, services, operations, or applicable laws and regulations. This assessment is documented, reviewed by senior management, and formally approved by the Board of Directors. It is updated regularly to reflect evolving threats and regulatory developments.

Client Risk Exposure

Customer behavior poses one of the primary risks of financial crime. The Company evaluates individual customer profiles by reviewing financial transparency, behavioral patterns, and connections to jurisdictions considered higher risk. Particular attention is given to Politically Exposed Persons (PEPs), customers with opaque sources of income, or those whose transactions appear inconsistent with declared financial circumstances.

- Customers assessed as low risk typically have verified and steady income, transparent activity, and limited exposure to high-risk factors.
- Customers classified as high risk may engage in high-value or erratic transactions, operate through complex financial structures, or have ties to regions with weak financial oversight. These cases require Enhanced Due Diligence (EDD) and closer monitoring.

Product, Service, and Transaction Risk

Certain services and transaction types carry a higher risk of financial abuse. For example, products involving cryptocurrencies, prepaid instruments, digital wallets, or peer-to-peer functionality may make it harder to trace the flow of funds.

To mitigate such risks, the Company deploys targeted controls, including:

- Real-time surveillance and automated flagging systems
- Transaction thresholds aligned to risk levels
- Alerts that detect unusual gaming or financial behavior

These controls are applied proportionally, based on the customer's individual risk profile.

Geographic Risk Factors

The geographic location of a customer or their financial activity plays a significant role in determining risk exposure. Customers linked to jurisdictions with weak AML/CFT frameworks, high levels of corruption, or international sanctions require more caution.

Risk assessments are informed by sources such as FATF, CFATF, OFAC, the European Commission, the US State Department, and Transparency International. Where elevated risks are identified, the Company applies:

- Mandatory Enhanced Due Diligence
- Manual review and approval of transactions
- Limits on services such as deposits or withdrawals

Distribution Channel Risk

The method by which customers access the Company's platform also affects risk exposure. Digital onboarding without face-to-face interaction increases vulnerability to fraud or identity misuse.

To address this, the Company implements safeguards such as:

- Biometric identity authentication
- Two-factor login procedures
- Secure digital document verification

These measures ensure that onboarding meets consistent compliance standards.

Technology-Related Risks

Before introducing new technologies or major system upgrades, the Company carries out a structured risk assessment. This process includes:

- Technical and operational evaluation
- Identification of security vulnerabilities
- Planning for appropriate mitigation measures
- Analysis of residual risk that may remain

This review applies to new game features, blockchain integrations, payment solutions, and other innovations. All assessments are documented and made available for inspection by relevant authorities when requested.

Industry-Specific Risks in Online Gaming

The Company recognises that online gaming carries certain risks that are unique to the sector. Criminal actors may attempt to exploit the platform through:

- Automated or high-frequency betting
- Abuse of promotions or bonuses
- Manipulating payouts to disguise criminal proceeds

To counter these tactics, the Company enforces:

- Restrictions on anonymous or unregulated payment methods
- Use of approved, regulated financial service providers
- Active monitoring of unusual gameplay patterns or coordinated player behavior

Risk Mitigation and Ongoing Controls

The Company mitigates identified risks through the implementation of proportionate and targeted controls. These measures are designed to strengthen customer oversight, maintain regulatory compliance, and ensure appropriate responses to risk signals. Common controls include:

- Requesting additional documentation from customers
- Restricting specific account functionalities where appropriate

- Applying enhanced monitoring procedures in accordance with the customer's risk rating

During the onboarding process, each customer and Payment Service Provider (PSP) is assigned an initial risk classification. These ratings are subject to regular review and may be updated based on new information or observed behavior.

Ongoing Screening and Monitoring

The Company conducts continuous monitoring of active customers to ensure alignment with their risk profile and to identify potential threats. This includes:

- Sanctions list screening against international and domestic watchlists
- Detection and review of Politically Exposed Person (PEP) status
- Adverse media checks using trusted information sources
- Evaluation of transaction patterns against established customer profiles

When alerts are triggered, the Compliance Department conducts a thorough review and initiates escalation or further investigation where warranted.

Documentation and Regulatory Reporting

The Company maintains secure and comprehensive records to demonstrate compliance with its Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing obligations. These records cover:

- Customer risk classifications and the rationale behind each decision
- Due diligence and enhanced due diligence procedures undertaken
- Monitoring activity logs and system-generated alerts
- Documentation of Business Risk Assessment (BRA) outcomes and revisions

If any behavior or transaction suggests potential financial crime, the Company reports the matter immediately to the Financial Intelligence Unit (FIU) of Curaçao. Disclosure of such reports or any form of tipping-off is strictly prohibited and considered a serious breach of compliance obligations.

Governance, Access, and Review

All internal risk assessments, including the BRA and Customer Risk Assessments (CRA), are thoroughly documented and retained in line with applicable requirements. These records include detailed breakdowns of both inherent and residual risk factors, segmented by customer type, product category, and geographic exposure.

Assessments are reviewed on a scheduled basis to ensure they remain current and effective. Upon request, they are made available to the Curaçao Gaming Control Board or any other competent authority for inspection.

7. Customer Due Diligence and Enhanced Due Diligence

The Company conducts a comprehensive evaluation of each prospective client before initiating a business relationship to ensure they do not present unacceptable risks relating to money laundering, terrorism financing, or the funding of weapons proliferation. This diligence is essential to protecting the platform's security and satisfying all applicable regulatory obligations.

Customer Due Diligence (CDD) represents the first layer of screening. It includes identity verification, assessment of financial and personal background, risk scoring, and ongoing surveillance for potential red flags. Information from publicly available sources, including employment data, property records, insolvency databases, and social media profiles, may be used to supplement this assessment.

When only limited risk indicators are identified, the Company applies standard due diligence. However, if elevated risk factors emerge such as links to high-risk jurisdictions or politically exposed persons (PEPs) then Enhanced Due Diligence (EDD) is required without exception.

Risk Scoring and Tools

The Company uses a formal scoring system that evaluates factors like location, financial behavior, transaction history, and platform usage. This is supported by automated tools and third-party solutions including LexisNexis, WorldCheck, and AI-driven monitoring systems. Biometric technologies and secure ID verification software are also utilized.

Anonymous or fictitious profiles are strictly prohibited. Every customer must submit verifiable identification, and any irregularities identified by the monitoring system are escalated to the Compliance Officer. This may result in regulatory reporting to the Financial Intelligence Unit (FIU) or notification to law enforcement authorities.

Clients are categorized as low, medium, or high risk, based on jurisdiction, transaction patterns, and funding sources. Relationships that exceed the Company's defined risk

threshold are rejected or terminated. Full criteria for risk classification are detailed in Appendix IV.

When Due Diligence Is Required

CDD procedures are activated in the following circumstances:

- When a transaction, whether individual or cumulative, reaches or exceeds NAF 4,000
- When there is suspicion of criminal or illicit financial activity
- When identification records are incomplete, inconsistent, or possibly falsified
- When small linked transactions collectively meet the legal threshold
- When customer behavior introduces new or higher risk factors

CDD includes:

- Verifying identity using reliable, independent documentation
- Identifying beneficial ownership and reviewing ownership structures (for corporate clients)
- Assessing company arrangements and applying appropriate scrutiny
- Monitoring customer behavior and transactions in line with the risk profile
- Verifying the origin of funds if additional concerns are identified
- Prioritizing internal reporting over continued verification in cases of suspected financial crime

Identity Verification Requirements

The Company collects the following from all customers:

- Full legal name
- Date and place of birth
- Residential address

- Nationality
- Government-issued ID number

Standard documentation suffices for low-risk clients. High-risk individuals must provide additional records to validate their financial profile. Accepted documentation includes:

- Valid passport or national ID
- Recent utility bill or bank statement for address verification
- Email, phone, or postal confirmation of address
- Biometric validation and IP address analysis
- Verification of payment method ownership

Where standard verification is insufficient, supplementary methods such as video-based checks or verification through the first deposit via a regulated financial institution are applied.

EDD involves further steps to verify source of funds, source of wealth, and to determine the customer's projected financial behavior. Employment or business-related documentation may be requested from medium and low-risk clients where necessary.

Timing and Limitations

CDD starts at registration. Core customer details are collected at sign-up and cross-checked against verified databases. If a single or cumulative transaction equals or exceeds NAF 4,000, the full CDD process must be completed.

If CDD is not completed within the required time:

- Deposits and withdrawals are paused until verification is concluded
- Withdrawal attempts result in a temporary account freeze
- After 30 days:
 - If suspicious activity exists, an STR is submitted to the FIU
 - If no red flags are detected, funds are returned to the source of deposit
 - If risks persist, the account may be closed

Employees are prohibited from informing clients about CDD reviews in progress. All CDD procedures are carried out discreetly, in full compliance with confidentiality rules.

Monitoring continues throughout the client relationship. The Company updates customer risk scores as new information emerges or behavior changes. CDD is reapplied in these situations:

- The customer's activity increases unusually
- The client relocates to a new jurisdiction
- A PEP designation is identified
- Cumulative transactions again meet NAF 4,000
- Regulatory changes affect due diligence requirements
- Legacy accounts that pre-date current standards and present elevated risk

If a client fails to comply with CDD requirements or is found to present excessive risk, the relationship is terminated. The Compliance Officer is responsible for approving such decisions, and suspicious conduct is reported immediately to the FIU.

Use of Third Parties in CDD

The Company may delegate certain CDD functions to vetted third-party providers. However, final responsibility for regulatory compliance remains with the Company.

Conditions for Third-Party Reliance:

- The third party must be subject to AML and CTF laws that are substantially equivalent to Curaçao's standards
- A formal agreement must require timely access to all relevant CDD data
- The Company must retain the right to audit or review the third party's performance
- The third party must perform CDD in its own capacity and not under the Company's direct instruction unless part of an outsourcing arrangement

Before engaging a third party, the Company evaluates:

- The provider's regulatory environment

- Its track record and technical capacity
- Its internal controls and data integrity measures

All data-sharing arrangements are governed by legal contracts, clearly defining responsibilities and protecting client confidentiality. Third parties are never authorized to make final decisions on onboarding or client rejection.

Beneficial Ownership Verification

When onboarding legal entities, the Company verifies the identity of the Ultimate Beneficial Owners (UBOs). This is essential for detecting hidden control structures and ensuring transparency.

Steps include:

- Identifying anyone who owns or controls 25% or more of the entity
- If no individual meets the threshold, identifying persons with operational control or significant influence
- Reviewing complex structures such as layered ownership or nominee arrangements
- Collecting documentation such as shareholder registries, company extracts, and organizational charts

If beneficial ownership cannot be conclusively determined, the most senior executive is designated as the UBO in line with FATF guidance.

The Company does not proceed with onboarding if the client delays or refuses to provide the required ownership or due diligence information. Such behavior is considered a red flag and may result in immediate termination of the relationship.

8. Customer Acceptance Policy

The Company has implemented a comprehensive Customer Acceptance Policy (CAP) to define how individuals and entities are evaluated and approved for access to its licensed online gaming and betting platform. This policy ensures robust protection against misuse for unlawful purposes, including but not limited to money laundering, terrorism financing, proliferation financing, fraud, sanctions evasion, and violations of

applicable laws. It also serves to uphold compliance with the regulatory framework governing gaming operators licensed in Curaçao.

The CAP forms an essential part of the Company's broader compliance program related to anti-money laundering (AML), counter-terrorism financing (CTF), and counter-proliferation financing (CPF). It incorporates the expectations of the Curaçao Gaming Control Board and reflects international benchmarks set by the Financial Action Task Force (FATF), the European Union AML Directives, and the Wolfsberg Group's best practices.

This policy is anchored in Curaçao's legal instruments, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

All personnel involved in client onboarding and management including directors, employees, contractors, and third-party providers must comply with this policy. No customer may deposit, place wagers, or initiate withdrawals before passing the required due diligence and receiving formal acceptance.

Scope and Coverage

The CAP applies to all individuals and legal entities attempting to register through any of the Company's access points, including the main website, mobile apps, affiliate platforms, or third-party integrations.

It remains applicable across the full duration of the customer relationship, from account creation to closure. The policy covers all services and games offered under the Company's gaming license (OGL/2024/511/0630).

Eligibility Criteria

Only persons or entities meeting legal eligibility requirements are permitted to register. Applicants must affirm that they are 18 years of age or older, subject to any applicable jurisdictional rules. Accurate and verifiable personal data is mandatory, including full name, date and place of birth, nationality, and a valid address.

Customers linked to jurisdictions under sanctions or categorized as high risk either internally or by external authorities are automatically rejected. Screening is conducted against global sanctions databases such as those maintained by the United Nations, European Union, OFAC, OFSI, and other relevant bodies.

All funds deposited by customers must originate from lawful and verifiable sources. Where elevated risk is detected, the Company may request documentation to verify the source of funds or wealth. Applications may be refused due to prior fraud, self-exclusion history, bonus exploitation, or regulatory violations.

Use of a Risk-Based Approach

The Company evaluates each applicant using a risk-based methodology at the point of registration. Risk assessments consider factors such as the applicant's occupation, transactional behavior, geographical exposure, and previous gambling activity.

- Low-risk customers show stable financial patterns and verifiable profiles
- High-risk customers may use opaque financial structures, display irregular transactions, or be associated with sensitive industries or high-risk regions
- PEPs and individuals closely associated with them are automatically classified as high risk

Enhanced Due Diligence (EDD)

For customers classified as high risk, the Company applies Enhanced Due Diligence, which includes additional verification requirements and continuous monitoring. EDD is triggered under the following conditions:

- Income or wealth cannot be reliably verified
- PEP involvement is identified
- Gambling behavior appears inconsistent with declared income
- Use of third-party or intermediary payment methods
- Duplicate or linked accounts are detected
- Sudden changes in customer behavior or transaction patterns
- Large withdrawals occur without corresponding gameplay

EDD involves verification of source of funds, limits on account activity, and review by senior compliance personnel.

Geographic Risk Evaluation

The Company assesses geographical risk based on the customer's place of residence, origin of funds, and the location of transaction activity. External references include FATF, CFATF, OFAC, the EU, the U.S. State Department, and Transparency International.

- Customers from countries under sanctions are automatically rejected

- Clients from high-risk jurisdictions must pass EDD and obtain clearance from compliance
- These accounts are subject to ongoing monitoring

Customer Risk Evaluation Process

The Company applies the following process for evaluating customer risk:

- Real-time screening during registration using global databases
- Assignment of a risk category (low, medium, high)
- Review and approval of high-risk customers by compliance staff
- Dynamic updates to customer risk scores based on behavior or changes in regulation

Product and Transaction Risk

Certain features and transaction types are recognized as higher risk, including:

- Peer-to-peer transactions and in-game transfers
- Anonymous payment methods or unregulated digital wallets
- Frequent deposits and withdrawals without proportional gameplay
- Payment methods not linked to the customer's verified identity

Only funds with a verifiable source are accepted. Suspect transactions are reported to the Financial Intelligence Unit (FIU). Transfers between customer accounts are restricted and require prior compliance review.

Channel and Technology Risk

Digital onboarding introduces impersonation and fraud risks. The Company has implemented the following measures to address these:

- Biometric ID checks
- IP and device location verification
- Multi-factor authentication for secure access

Before adopting any new technology or payment option, a formal risk assessment is conducted. Tools that may obscure identity are subject to heightened scrutiny. Third-party partners involved in onboarding or payment processing must meet rigorous compliance and transparency standards.

Risk Dimensions and Indicators

The Company uses a multi-dimensional approach to assess risk across the following areas:

1. **Customer Profile Risk:** Includes frequent turnover, use of intermediaries, duplicate accounts, inconsistent income declarations, or links to junket operations
2. **Product and Transaction Risk:** Covers anonymous payments, inconsistencies in identification documents, third-party deposits, and high-frequency switching of payment methods
3. **Geographic Risk:** Relates to customers or transactions tied to high-risk or sanctioned countries
4. **Channel and Technology Risk:** Involves onboarding via unverified channels or usage of unauthorized third-party systems

Risk Scoring and Control Measures

A risk calculator is used to assign customers a risk score. Controls are applied according to the assigned risk tier:

- **Low Risk:** Standard due diligence is required
- **Medium Risk:** Additional documentation and closer monitoring apply
- **High Risk:** Enhanced due diligence is triggered, including senior compliance approval and continuous surveillance

Customer risk levels are continuously re-evaluated and adjusted based on behavioral patterns, regulatory updates, and internal reassessments.

Risk Indicators Reference Table:

Risk Factor	Low Risk	Medium Risk	High Risk
-------------	----------	-------------	-----------

Purpose of Account	Recreational or casual gambling	Consistent high-stakes or professional play	Bonus abuse, financial misuse, or exploitation of platform incentives
Source of Funds	Salary, pension, or other regular income	Business income, asset sales, or inheritance	Unverifiable crypto assets, offshore funds, or unclear origin of income
Source of Wealth	Employment, verified investments, or inheritance	Sale of property or a business	High-risk ventures, offshore holdings, or unverifiable wealth
Transaction Frequency	Occasional	Weekly	Daily or multiple times per day
Transaction Value	Up to NAF 1,000	Between NAF 1,000 and NAF 4,000	Above NAF 4,000
Incoming Payments	Debit/credit cards or standard bank transfers	Prepaid cards or e-wallets	Crypto deposits, third-party funding, or transfers from high-risk countries
Outgoing Payments	Regular withdrawals or standard refunds	Bonus-related or frequent small withdrawals	Crypto withdrawals, chargebacks, or suspicious cash-out activity
Gaming Behaviour	Moderate and consistent betting activity	High-stakes play or long-duration sessions	Aggressive betting, collusion, multiple

			accounts, or erratic activity
Payment Channels	Traditional bank transfers	Verified digital wallets	Anonymous or lightly regulated tools
Adverse Media	No negative media coverage	Unconfirmed adverse references or allegations	Verified links to criminal activity or illicit operations

Application of Risk Indicators

The Company applies predefined risk indicators during the client lifecycle, including at onboarding, during ongoing monitoring, and throughout periodic reviews. Each risk factor is evaluated independently, followed by a holistic analysis to determine the customer's overall risk classification.

- Clients showing predominantly low-risk features are processed under standard due diligence.
- Where there is a mix of low- and medium-risk elements, additional verifications are required and monitoring is increased proportionally.
- If one or more high-risk indicators are identified, Enhanced Due Diligence (EDD) is mandatory. In such cases, services are withheld until the EDD process is completed and approved by senior compliance staff.

Risk classifications are dynamic. They are periodically reviewed and updated in response to behavioral changes, regulatory updates, alerts, or external intelligence. This ongoing reassessment allows the Company to stay aligned with current threat landscapes and maintain regulatory compliance.

Onboarding Procedures

The Company employs a well-structured and fully documented onboarding process that ensures only customers who meet its compliance, regulatory, and risk criteria are granted access to its gaming services. No user account is activated unless all steps identity verification, documentation review, and sanctions screening are finalized.

Registration and Identification Requirements

Each prospective customer is required to submit accurate and verifiable personal data, including:

- Legal full name
- Date and place of birth
- Nationality
- Residential address
- Government-issued identification number (e.g., ID card or passport)

Automated systems screen all applicants against sanctions lists and databases identifying Politically Exposed Persons (PEPs). Any matches are escalated to compliance officers for manual evaluation.

Customers classified as high risk must undergo enhanced verification. Depending on the case, supporting documents may include:

- Recent bank statements demonstrating income patterns
- Payslips or income tax returns
- Proof of ownership of assets (e.g., real estate or investments)
- Contracts evidencing major asset sales
- Investment account summaries

Identity and Verification Requirements

The Company enforces strict standards for verifying client identity, which apply equally to individuals, beneficial owners, and authorized representatives.

Objectives of Document Verification

Verification procedures are designed to prevent the following:

- Use of counterfeit or manipulated identity documents
- Impersonation or identity theft
- Submission of altered screenshots or edited files

Documents must include:

- Full legal name
- Complete date of birth
- Identification number
- Issue or expiry date
- A visible photograph
- Signature, if applicable

All identification must remain valid for at least one month beyond submission and be submitted in full, legible, and undamaged format.

Upload and Document Validation Standards

Documents must meet the following requirements:

- Accepted file types: JPG, JPEG, PNG, PDF
- Must be in color
- Both front and back if applicable
- Minimum resolution: 300 DPI or 100 KB file size
- All document corners must be clearly visible
- No screenshots or files altered digitally
- Digital-only documents are allowed only with prior approval

Image Authenticity Verification

Automated tools are used to confirm the authenticity of submitted files, including:

- Analysis of metadata and file structure
- Detection of editing or tampering software
- Risk-based image tampering scoring
- Comparison with official document templates
- Review of font types and document layout

Extracted data is cross-referenced with both internal databases and external verification services.

Proof of Address Verification

In-Person Clients

When onboarding occurs in person, the Money Laundering Compliance Officer (MLCO) reviews the original PoA document and retains a certified copy for the records.

Remote Clients

For online clients, the PoA process includes:

- Submission of a document issued within the last 90 days
- System-based checks to confirm authenticity and format
- Digital trust scoring and geolocation validation (e.g., via Google Maps)
- Manual review by compliance for additional verification

Accepted documents include:

- Utility bills (electricity, water, broadband)
- Bank or credit card statements
- Tax letters, mortgage statements, lease agreements
- Employer-issued letters or government-issued correspondence
- Voter registration or real estate title documentation

Documents that include full address and may also be accepted:

- Passport
- National ID
- Driving license
- EU-issued residence permit

Documents not accepted:

- Mobile phone bills
- Prepaid card records
- Medical bills or insurance statements
- Documents listing only a P.O. Box
- Records older than 90 days

A single document cannot be used for both identity and address verification.

Source of Funds (SOF) and Source of Wealth (SOW)

- **Source of Funds (SOF)** refers to the origin of the specific financial assets used for transactions on the platform, such as deposits.
- **Source of Wealth (SOW)** encompasses the customer's overall financial background, including employment income, business ownership, investments, or inheritance.

Both SOF and SOW must be documented where risk levels justify additional scrutiny. For high-risk clients, formal verification is required prior to allowing significant transactions or withdrawals.

The Company requires documentation to support the declared SOF and SOW, such as:

Income Type	Documentation Examples
Employment income	Payslips, income tax returns, bank statements
Inheritance	Probate letters, wills, confirmation from legal professionals
Gifts or Donations	Notarized declarations, signed gift agreements

Savings	Bank savings statements showing a consistent accumulation history
Government grants	Grant approval letters, benefit statements from relevant authorities
Dividends or Profits	Dividend statements, audited financial reports
Loans or Investments	Loan agreements, transfer receipts, investment confirmations
Property or Asset Sales	Sales contracts, dealer confirmations, shipping documents, or customs declarations

These documents must demonstrate a clear and legitimate link between the customer and the funds involved, supporting full transparency and traceability in accordance with applicable AML and CTF regulations.

Ongoing Monitoring

The Company recognises that customer onboarding is merely the initial phase of an effective compliance framework. Ongoing due diligence is essential to ensure that customers continue to behave in accordance with their assigned risk category, and to identify any developments that may increase the risk of financial crime.

Real-Time Monitoring

To ensure continuous oversight, the Company uses automated monitoring systems capable of analysing customer activity in real time. These tools are designed to detect unusual or potentially suspicious behaviour that may suggest platform misuse. The following triggers may initiate alerts:

- Activity that differs significantly from the customer's established transaction pattern
- Rapid movement of funds with minimal or no gaming engagement

- Use of unfamiliar or irregular payment methods, or frequent changes to those instruments
- Patterns indicative of collusion, bonus abuse, or transactions lacking a clear economic purpose

When an alert is generated, it is forwarded to trained compliance personnel for review. Where appropriate, further investigation is conducted, and internal procedures are followed, including potential escalation or regulatory reporting.

Periodic Risk-Based Reviews

In addition to real-time alerts, the Company performs scheduled customer reviews based on risk categorisation. These periodic assessments are used to:

- Confirm the validity and currency of Know Your Customer (KYC) and risk-related information
- Detect behavioural changes that could warrant a revised risk classification
- Apply further due diligence where circumstances require it

Reassessment is triggered when:

- A customer begins transacting from or relocates to a high-risk jurisdiction
- There is a significant increase in deposits, betting activity, or withdrawals
- New funding sources are detected, particularly those from unregulated or third-party origins

If any of the above occur, the customer's risk profile is reassessed, and additional documentation may be requested. Temporary limitations may be placed on the account until verification is completed.

Prohibited Clients and Transaction Scenarios

To protect operational integrity and uphold compliance standards, the Company maintains strict prohibitions against onboarding certain customer types or processing specific transactions.

Unacceptable Conditions for Onboarding or Continued Service

The Company refuses to onboard or provide ongoing service in any of the following cases:

- The individual fails or refuses to provide required identification or verification documents, without a legitimate and documented reason for delay
- The customer is listed on a financial sanctions list or recognised watchlist, including those maintained by the United Nations, European Union, OFAC, OFSI, or Curaçao regulatory authorities
- The transaction involves a financial institution based in a jurisdiction with inadequate regulatory oversight, or through entities such as shell banks or anonymous accounts

Customers are also barred from participation where there is evidence or suspicion of:

- Involvement in terrorism as defined by European Union legislation
- Engagement in drug trafficking under the 1988 United Nations Convention
- Links to organised crime, human trafficking, or cybercrime
- Participation in fraud, corruption, currency forgery, or tax-related crimes

Immediate Rejection and Exclusion Criteria

The Company applies immediate rejection of applications or account suspension under the following conditions:

- The individual is anonymous, fails to verify their identity within 30 days, or submits fraudulent or unverifiable documentation
- The customer transacts using bearer instruments or engages in high-risk sectors such as arms trading, adult entertainment, or unlicensed virtual asset services
- The customer resides in, or transacts from, jurisdictions classified as prohibited or sanctioned
- The individual is under the minimum legal gambling age or provides false eligibility information
- There is evidence of collusion, abuse of promotional features, manipulation of gaming functionality, or use of stolen identities
- The source of funds or overall wealth is unverifiable or suspected to derive from unlawful activity

Prohibited Jurisdictions

In line with its internal compliance standards and applicable legal obligations, the Company enforces a strict prohibition on customer registrations and transactions from specific jurisdictions. This includes both unrecognised territories and countries designated as high-risk, sanctioned, or otherwise incompatible with the Company's compliance obligations.

Unrecognised or Disputed Territories

The Company does not establish business relationships with persons located in or associated with the following areas:

- Crimea
- Donetsk
- Luhansk
- Republic of Abkhazia
- Republic of South Ossetia
- Nagorno Karabakh
- Turkish Republic of Northern Cyprus
- Palestine
- Kosovo
- Pridnestrovian Moldavian Republic
- Somaliland

Prohibited Countries

The Company rejects all registrations and transactions from the countries listed below:

- Australia
- Belarus
- Belize
- Central African Republic
- Cuba
- Curaçao
- Democratic Republic of Congo
- Dutch West Indies (Aruba, Bonaire)
- France
- Germany
- Iran
- Iraq
- Lebanon
- Libya
- Mali
- Netherlands
- North Korea
- Russia

- Somalia
- Sudan
- Syria
- United Kingdom
- United States
- Yemen

All applications originating from these jurisdictions are automatically declined during onboarding, and any attempted transactions are blocked in real time. The Company retains logs of these rejections to meet its regulatory reporting requirements under Curaçao law.

Enhanced Due Diligence and Escalation Procedures

Customers identified as presenting a higher financial crime risk are subject to Enhanced Due Diligence (EDD). This applies in particular to Politically Exposed Persons (PEPs), individuals with ties to high-risk jurisdictions, or customers displaying behaviour inconsistent with their known financial circumstances.

EDD includes the following measures:

- A comprehensive review of the customer's financial background
- Verification of source of funds and source of wealth using trusted documentation
- Collection of supporting documents, which may include:
 - Financial statements
 - Tax returns and payslips
 - Contracts from asset sales
 - Investment portfolio records
 - Proof of beneficial ownership for legal entities

All EDD cases must be approved by senior compliance personnel. Where appropriate, high-risk cases are escalated to the Board of Directors. Once approved, these customers are subject to:

- Lower thresholds for transaction review
- Increased frequency of risk reassessments

- Ongoing monitoring through automated alerts

This tiered approach enables the Company to mitigate financial crime risks effectively and maintain compliance with Curaçao's legal and regulatory requirements.

Prohibited Categories of Customers

The Company maintains a zero-tolerance policy toward onboarding or servicing customers who pose an unacceptable legal, financial, regulatory, or reputational threat. The following customer categories are explicitly barred:

- Individuals using false, anonymous, or misleading identities
- Customers who do not complete identity verification within 30 days
- Legal entities with shell structures or unverifiable ownership
- Persons or entities appearing on international or domestic sanctions lists
- Residents of, or transactors from, restricted or prohibited jurisdictions
- Underage individuals who do not meet the legal minimum gambling age
- Customers with a history of fraud, identity theft, bonus abuse, or suspicious conduct
- Users who fund accounts using unverified third-party sources or anonymous methods
- Individuals whose source of funds or wealth cannot be verified reliably

Triggers for Immediate Rejection or Suspension

The Company may reject a customer application or suspend an active account under any of the following conditions:

Identity and Documentation Triggers:

- Failure to provide valid Know Your Customer (KYC) documentation or proof of address
- Submission of forged, tampered, or suspicious documentation
- Failure to respond during the verification process

AML, CTF, and CPF Risk Triggers:

- Match with PEP or sanctions databases without adequate mitigation
- Indicators of direct or indirect involvement in financial crime
- Inability to demonstrate a legitimate source of funds

Behavioural and Transactional Red Flags:

- Financial activity that contradicts the declared customer profile
- Use of multiple accounts, third-party transactions, or unsupported payment tools
- Attempts to bypass controls, manipulate platform features, or engage in coordinated fraud
- Repeated abuse of promotions or other gameplay anomalies

Termination of Customer Relationships

The Company reserves the right to terminate any customer relationship to preserve regulatory compliance and platform integrity. Reasons for termination include but are not limited to:

- Failure to provide required documentation within specified timeframes
- Confirmed or suspected involvement in money laundering, terrorist financing, or proliferation financing
- Breaches of Curaçao's gaming laws or Responsible Gambling Policy
- Residency in or connection to a prohibited jurisdiction
- Submission of false or misleading information
- Financial behaviour inconsistent with the declared income or background
- PEP designation where associated risks cannot be mitigated
- Use of payment instruments not registered in the customer's name
- Underage activity or fraudulent misrepresentation

If the termination involves suspected financial crime, a Suspicious Transaction Report (STR) is submitted to the Financial Intelligence Unit (FIU) Curaçao under the National

Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds are returned to the original funding source, unless subject to seizure or freeze orders.

Termination-related documentation and evidence are securely retained for a minimum period of five years.

Legal and Regulatory Compliance

This Customer Acceptance Policy forms a core component of the Company's AML, CTF, and CPF compliance architecture and is fully consistent with the following Curaçao laws and regulations:

- The National Ordinance on Identification when Rendering Services (NOIS)
- The National Ordinance on the Reporting of Unusual Transactions (NORUT)
- The Sanctions National Ordinance (SNO)
- The Kingdom Sanction Act
- The National Ordinance on Games of Chance (LOK)

These frameworks are embedded in the Company's end-to-end customer management processes.

Responsible Gambling Integration

The Company's Customer Acceptance Policy is aligned with its Responsible Gambling framework. Where customer behaviour suggests signs of harm or elevated financial risk, the Company initiates immediate interventions, which may include:

- Imposing temporary deposit or loss limits
- Restricting access to higher-risk gambling services
- Suspending or closing customer accounts
- Enforcing self-exclusion across platforms

Support staff and customer-facing teams are trained to recognise signs of gambling-related harm and follow established escalation protocols.

Policy Oversight and Recordkeeping

This policy is reviewed at least once a year to ensure consistency with legal requirements, risk exposure, and best practices. The Compliance Officer leads the review, which is submitted to the Board of Directors for approval.

All records relating to the Customer Acceptance Policy are stored securely for at least five years after account closure. These include:

- Identity verification data
- Address verification and source of funds documentation
- Risk assessment reports and due diligence logs
- Monitoring alerts and investigation notes
- EDD files and account closure records

Access to these records is restricted to authorised personnel and monitored in line with the Company's data protection policies.

9. Transaction Monitoring

Overview

The Company considers transaction monitoring a fundamental component of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) strategy. Given the dynamic and high-volume nature of online gaming operations, the potential for misuse by bad actors is significant. To address this risk, the Company maintains an integrated monitoring system that actively evaluates transactions in real time and supports early identification of unusual or suspicious behavior.

Regulatory Compliance

The Company's monitoring procedures are fully aligned with Curaçao's legal framework, including obligations under the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the Sanctions National Ordinance (SNO). All processes reflect the expectations of the Financial Intelligence Unit (FIU Curaçao) and support timely submission of required reports and escalation of concerns.

Monitoring Framework and System Design

The monitoring system is built on a dual-layered approach combining automation and human oversight. Machine learning models and rule-based detection engines are used to analyze behavior, assess risk scores, and generate alerts for anomalous activity. All flagged alerts are reviewed by the Compliance Department to determine whether further investigation or escalation is required.

Key red flags and risk indicators include:

- Deposits that are unusually large or inconsistent with the customer's known profile
- Use of multiple or opaque payment instruments, particularly those offering anonymity
- Quick movement of funds into and out of accounts with little to no gameplay
- Fund transfers between linked or associated accounts
- Transactions involving jurisdictions with weak AML enforcement or high secrecy levels

Risk-Based Configuration and Threshold Triggers

Each transaction is assessed based on the customer's assigned risk rating. Parameters such as transaction value, payment method, customer behavior, and geographic exposure are considered.

Transactions that trigger further review include:

- Any transaction, or series of linked transactions, equal to or exceeding NAF 4,000
- Repetitive or high-frequency financial activity
- Activity that is inconsistent with declared income or known financial behavior
- Logins from IP addresses that do not match the customer's declared location
- Access or transactions involving prohibited or high-risk jurisdictions

Where a customer reaches the NAF 4,000 threshold, a full Customer Due Diligence (CDD) review is triggered, including document re-verification if necessary.

Analytical Tools and Review Techniques

To improve effectiveness, the Company employs a wide range of analytical and technical measures such as:

- Geolocation filtering to detect access from blocked or suspicious regions
- IP address matching and device fingerprinting to identify linked accounts
- Velocity controls to flag rapid and unusual financial flows

- Income-to-activity comparisons to assess fund legitimacy
- Gaming pattern analysis to detect deviations from normal behavior

The platform aggregates data across all sessions, transactions, and customer activity to create a behavioral baseline for each user, which is continuously monitored for deviations.

Escalation and Reporting Protocols

When an alert is deemed credible, an internal Suspicious Activity Report (SAR) is created and escalated to the AML/CTF Officer. If further investigation confirms the presence of suspicious activity, a formal Suspicious Transaction Report (STR) is submitted to the FIU Curaçao in accordance with the NORUT.

All monitoring records, alerts, decisions, and STR filings are timestamped, stored securely, and retained for regulatory audit and inspection purposes.

Account Freezing and Termination

If the Company is unable to complete the required CDD or Enhanced Due Diligence (EDD) due to missing or unverified documentation, the customer account is frozen. Unless otherwise ordered by a regulatory or judicial authority, any remaining funds are returned to the original payment method. In the case of suspected criminal activity, the business relationship is terminated, and the matter is escalated to the appropriate regulatory body.

10. Politically Exposed Persons

Risk Awareness and Policy Commitment

The Company recognises that customers who qualify as Politically Exposed Persons (PEPs) present an increased risk of involvement in financial crime, particularly regarding corruption and money laundering. In line with its risk-based compliance framework, the Company applies strict Enhanced Due Diligence (EDD) measures to any customer identified as a PEP or closely associated with one.

Definition and Scope

A Politically Exposed Person refers to an individual who currently holds or has recently held a prominent public position. This includes, but is not limited to:

- Heads of state or government

- Senior politicians or members of legislative bodies
- High-ranking judicial or military officials
- Senior executives of state-owned enterprises
- Officials within major international organisations

In addition to these individuals, the following are treated with the same level of scrutiny:

- Immediate family members of PEPs
- Close personal or professional associates of PEPs

Onboarding Controls and Senior Management Approval

If a PEP is identified during account registration or through ongoing monitoring, the Company initiates a structured risk evaluation process. This process includes:

- A thorough assessment of the customer's profile and potential risk exposure
- Verification of the customer's declared source of wealth and income
- Collection of documentation supporting financial background and asset ownership
- Mandatory written approval from senior management prior to account activation

Under no circumstances will an account linked to a PEP be opened or maintained without prior documented approval from a senior-level manager.

Internal Register and Recordkeeping

The Compliance Officer maintains a dedicated internal register of all confirmed PEPs. This register contains:

- Full identification details of the individual
- Results of the risk assessment
- All mitigating actions taken
- Supporting documents used to justify the decision to approve the business relationship

This register is regularly reviewed and updated to reflect any changes in the customer's risk status, occupation, or associated relationships.

Monitoring and Risk Management

Customers identified as PEPs are monitored more closely than standard account holders. Ongoing measures include:

- Continuous monitoring of financial activity for unusual behavior
- More frequent reassessments of risk level
- Lower thresholds for triggering internal alerts or reviews

These controls ensure full alignment with the regulatory standards in Curaçao and international frameworks such as those issued by the Financial Action Task Force (FATF). The Company's proactive approach helps safeguard its platform from reputational damage, legal liability, and regulatory enforcement action stemming from associations with politically exposed individuals.

11. Sanctions Policy

Commitment to Sanctions Compliance

The Company fully complies with all relevant international sanctions laws and regulatory frameworks. This policy outlines the internal procedures and safeguards in place to detect, mitigate, and prevent any interaction with sanctioned parties, whether individuals, legal entities, or jurisdictions. Sanctions are imposed by authorities to achieve foreign policy objectives, combat financial crime, and enforce rules on terrorism, human rights, and corruption.

Categories of Sanctions

Sanctions may take multiple forms depending on the issuing body. The Company recognises the following categories:

- **Comprehensive sanctions:** Apply blanket prohibitions on trade or financial dealings with certain jurisdictions
- **Regime-focused sanctions:** Target political or state-linked actors involved in destabilising or unlawful conduct
- **Sectoral sanctions:** Affect specific industries such as energy, finance, or defense

- **Debt and equity restrictions:** Limit the issuance or trading of financial instruments associated with sanctioned entities
- **Conduct-based sanctions:** Directed at individuals or organisations involved in terrorism, cybercrime, arms trafficking, or other serious offences

Sanctions programs often combine these categories depending on policy objectives.

Sanctions Regimes Applicable to the Company

The Company ensures full compliance with the following regulatory frameworks:

- **United Nations (UN):** Binding on all member states and integrated into screening processes
- **European Union (EU):** Applicable to EU nationals and entities, regardless of location, and to any activity linked to the EU
- **United Kingdom (UK):** Applies to UK nationals, residents, companies, and operations involving UK jurisdiction
- **United States (US):** Includes primary and secondary sanctions. The Company adheres to US regulations where legally permissible, and escalates any legal conflict (such as with the EU Blocking Statute) to senior management for resolution

Core Compliance Principles

The Company commits to the following:

- Blocking or freezing assets where legally mandated
- Rejecting transactions or onboarding attempts involving sanctioned persons or locations
- Preventing the circumvention or evasion of sanctions
- Integrating sanctions controls into customer onboarding, transaction monitoring, and risk assessments
- Terminating relationships if sanctions obligations cannot be satisfied

Consequences of Non-Compliance

Violations may result in criminal prosecution, administrative penalties, and reputational harm. Employees found in breach of this policy are subject to disciplinary action.

Roles and Responsibilities

Board of Directors

Responsible for approving the sanctions policy, allocating compliance resources, and overseeing policy effectiveness.

Directors

Support decision-making on high-risk sanctions cases and jurisdictional issues.

Compliance Officer

Manages daily implementation of the sanctions framework, including:

- Sanctions risk assessments
- Policy updates and staff guidance
- Screening tool oversight
- Investigation and escalation of sanctions matches

All Employees

Expected to adhere strictly to the policy, complete training, report concerns, and never assist customers in avoiding sanctions.

Sanctions Screening Processes

All customers are screened during onboarding and throughout the business relationship using real-time data feeds from third-party providers. Screening covers:

- EU consolidated sanctions lists
- UK lists from HM Treasury and other relevant authorities
- US lists from OFAC, BIS, and other federal bodies
- UN Security Council consolidated list

Screening matches are categorised as:

- True positives
- Potential matches

- False positives
- Non-criminal listings
- Unknown status (pending investigation)

All potential and confirmed matches are escalated for further review by the Compliance Officer.

Handling of Confirmed Matches

If a customer or transaction is confirmed to relate to a sanctioned person or jurisdiction, the Company takes appropriate steps such as:

- Blocking or freezing the funds
- Terminating the relationship
- Restricting future transactions
- Notifying authorities when required
- Documenting the rationale and outcomes in detail

Sanctions Evasion Prevention

Evasion attempts are actively monitored and prohibited. This includes:

- Structuring transactions to conceal sanctioned links
- Use of intermediaries or anonymous entities
- Altering payment or identity information
- Accessing the platform via VPNs to mask prohibited jurisdictions

All suspicious behaviour is escalated internally and subject to compliance investigation.

Asset Freezing Obligations

When legal obligations require the freezing of assets, the Company acts immediately. Frozen assets remain the property of the client but are inaccessible and cannot be used or transferred without regulatory clearance. This applies to fiat currency and digital assets.

Sanctions Compliance Training

All staff undergo annual sanctions training. Specific departments such as onboarding, payments, and risk also receive tailored training modules. Training covers:

- Core features of global sanctions regimes
- Common evasion methods and red flags
- Internal obligations and escalation procedures
- Legal implications of non-compliance

New employees must complete initial training within 30 days of hire. All training records are documented and securely retained.

Third-Party Sanctions Screening

The Company may engage third-party providers for sanctions-related services. However, it retains full responsibility for the effectiveness and legal compliance of all outsourced activities. Prior to engagement, due diligence is conducted to assess technical capability, governance structures, and regulatory history. The Compliance Officer maintains oversight of all third-party activities.

Recordkeeping Requirements

The Company securely retains all sanctions-related records for at least five years following the termination of the business relationship or final relevant activity. This includes:

- Screening results and investigations
- Reports to regulators
- Internal review documents
- Staff training and attendance logs
- Escalation notes and approvals

These records are stored securely with access limited to authorised personnel. Access activity is logged and monitored. The retention period is a minimum of five years from the end of the business relationship or the date of the last relevant activity, whichever is later.

12. Suspicious and Unusual Activity & Transaction Reporting

The Company recognises the identification and reporting of suspicious or unusual activities as a critical element of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) programme. This obligation plays a vital role in preventing misuse of the platform and maintaining compliance with applicable laws and regulations in Curaçao.

Timely detection and accurate reporting help safeguard the Company from legal and reputational risks while also contributing to the broader efforts of financial crime prevention. Any failure to submit a report whether due to negligence or deliberate inaction may result in regulatory penalties, reputational damage, or criminal prosecution.

Detection of Suspicious and Unusual Conduct

Suspicious or unusual activity may be detected through the automated transaction monitoring system or observed directly by staff. Common indicators include:

- Large, fragmented, or unstructured deposits and withdrawals
- Sudden or unexplained changes in transactional behavior
- Wagering activity that appears inconsistent with normal gameplay
- Use of the account in a way that does not match the customer's known risk profile
- Efforts to obscure the origin or flow of funds, especially through intermediaries or third parties

While these behaviors may not always imply criminal intent, they must be evaluated promptly and thoroughly in line with internal procedures.

Internal Review and Escalation Process

A structured, two-stage review mechanism governs how potential suspicious activities are managed:

1. Preliminary Assessment

Activities flagged by the Company's monitoring systems or reported by staff undergo an initial assessment to determine whether there is a plausible explanation or if the activity warrants escalation.

2. Formal Review by AML/CTF Officer

If suspicion remains, a formal internal Suspicious Activity Report (SAR) is submitted to the designated AML/CTF Officer. The Officer then evaluates whether a report must be escalated to the Financial Intelligence Unit (FIU) of Curaçao.

All reports and findings are documented and stored securely in accordance with AML recordkeeping obligations.

Filing Unusual Transaction Reports (UTRs)

Under Article 1 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is obligated to file Unusual Transaction Reports (UTRs) with the FIU Curaçao using the goAML reporting platform. This obligation has been in effect since 1 January 2021 and applies to all operators of online gambling services licensed in Curaçao.

The AML/CTF Officer is responsible for:

- Determining whether the unusual activity meets the threshold for mandatory reporting
- Submitting UTRs via the goAML platform within regulatory timeframes
- Maintaining internal records of the submission, including justification and supporting documentation
- Ensuring all relevant personnel adhere to the internal reporting procedures defined under this Policy

If the nature or seriousness of the activity justifies it, the customer's account may be suspended or closed while further investigation is conducted.

Employee Reporting Responsibilities

Every employee has a duty to report any concern or suspicion regarding potential involvement in money laundering, terrorism financing, or related illicit conduct. This duty applies even when the suspicion is based on limited information or incomplete context.

Reports must be submitted immediately to the AML/CTF Officer via designated internal reporting channels. Upon receiving a report, the Officer determines:

- Whether additional facts or clarification are needed
- Whether the case warrants filing with the FIU Curaçao
- What immediate steps should be taken to mitigate potential exposure or prevent further risk

Suspicious and Unusual Activity

The Company monitors both transaction behavior and inconsistencies in customer profiles to identify activity that may be suspicious. A range of red flags may trigger internal investigation, including:

- Repeated use of anonymous funding methods such as prepaid cards or vouchers

- Mismatches between the customer's physical location and the origin of their financial transactions
- Large deposits followed by immediate withdrawal requests, without any meaningful gaming activity
- Requests to withdraw funds using payment methods registered to third parties
- Attempts to avoid verification procedures, or the use of false or proxy identities
- Spending patterns that contradict the customer's declared financial situation
- Frequent or unexplained updates to account ownership information
- Reluctance or failure to provide required due diligence documents

Each flagged case is recorded in detail, including timestamps, transaction types, financial values, and associated customer data. The Compliance and Fraud Prevention teams conduct a thorough review of the customer's full profile and all relevant evidence to determine whether escalation or formal reporting is necessary.

Suspicious and Unusual Transactions

A transaction may be considered unusual when it deviates significantly from the customer's expected financial behavior or known economic background, particularly when no lawful justification is provided. Examples include:

- Abrupt increases in deposit or withdrawal volumes without clear explanation
- Use of third-party accounts or connections to previously unassociated individuals
- Transactional patterns that appear inconsistent with the customer's stated income or wealth

The Company operates a real-time transaction monitoring system designed to detect these anomalies. When triggered, alerts are forwarded directly to the Compliance Officer for review. In parallel, employees are trained to recognize and report these types of behavioral and transactional warning signs through the internal escalation channels.

Types of Transactions Requiring Enhanced Scrutiny

Certain transactions are inherently high-risk and must undergo detailed assessment. These include:

- Transactions previously flagged or reported due to suspicion of links to money laundering or terrorist financing
- Activity involving customers or entities identified on the Sanctions National Ordinance or other equivalent watchlists
- Any transaction, or group of transactions within 24 hours, that amounts to 5,000 Netherlands Antillean Guilders (NAF) or more, whether related to deposits, bets, or withdrawals

Where reasonable suspicion exists that a transaction may be connected to money laundering, terrorism financing, or proliferation financing, immediate escalation to the Compliance function is mandatory. Timely review ensures risks are addressed and that reporting obligations are met.

Timely Reporting

Once a transaction has been assessed and determined to be suspicious or unusual, the Company must promptly submit an Unusual Transaction Report (UTR) to the Financial Intelligence Unit (FIU) of Curaçao, in accordance with AML Regulation IV.1. This requirement applies even if the transaction is only attempted and not completed.

The Compliance Officer is solely responsible for filing such reports and may do so without requiring further internal approval. Delayed submissions are considered a breach of regulatory compliance and may expose the Company to legal consequences.

Confidentiality and Reporting Culture

All information related to Suspicious Activity Reports (SARs) and Unusual Transaction Reports (UTRs) is strictly confidential. Staff are expressly prohibited from disclosing the existence, status, or content of such reports to the customer concerned or to any unauthorized party.

Any breach of this confidentiality may constitute "tipping-off" under Curaçao law and can interfere with regulatory investigations. Access to SAR-related information is restricted to the Compliance Officer and a limited group of approved personnel.

To support this standard, the Company incorporates targeted training on SAR confidentiality into its AML and CTF employee education programs. Any violation of this confidentiality policy is treated as a serious compliance matter and may result in disciplinary action, up to and including termination of employment.

Commitment to a Strong Reporting Culture

The Company fosters a workplace culture grounded in vigilance, confidentiality, and accountability. This approach strengthens the effectiveness of its AML, CTF, and CPF

program, supports compliance with Curaçao's legal framework, and reinforces its role in the global effort to combat financial crime within the gaming sector.

13. Compliance Officer

The Company designates a dedicated Compliance Officer who also acts as the Money Laundering Reporting Officer (MLRO). This individual holds primary responsibility for managing the Company's Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework.

This position operates independently from operational and commercial teams to ensure unbiased oversight. The Compliance Officer is granted unrestricted access to all internal systems, customer data, transaction records, and relevant personnel. In accordance with Regulation V.3 of the Curaçao Gaming Authority's AML Guidelines, the Compliance Officer reports directly to the Board of Directors.

Key Areas of Responsibility

Regulatory Contact and Reporting

The Compliance Officer serves as the Company's lead liaison with regulatory bodies, including the Financial Intelligence Unit (FIU) of Curaçao. Core responsibilities in this area include:

- Filing Suspicious Activity Reports (SARs) via the goAML system
- Responding to regulatory audits, inspections, and compliance-related inquiries
- Delivering quarterly reports to the Board highlighting risks, control updates, and policy developments

Oversight of Compliance Framework

This role includes implementation and supervision of the Company's AML, CTF, and CPF policies. The Compliance Officer ensures that all internal controls:

- Comply with national regulations and international guidance
- Reflect evolving regulatory expectations and risk exposures
- Are consistently enforced across all departments

Transaction Oversight and Case Investigation

The Compliance Officer is responsible for managing both automated and manual monitoring processes. Specific tasks include:

- Reviewing alerts generated by transaction monitoring systems
- Investigating any internal reports concerning potentially suspicious activity
- Determining the need and timing for reporting to the FIU
- Ensuring all investigations and findings are comprehensively documented

Employee Training and Awareness

The Compliance Officer coordinates the Company's compliance training program, which includes:

- Tailored training for onboarding teams, risk analysts, and customer support staff
- Mandatory annual training for all employees
- Updates to materials based on legislative changes or identified internal weaknesses

Internal Reviews and Risk Evaluation

To ensure a responsive and adaptive compliance system, the Compliance Officer also:

- Carries out regular audits of the Company's AML controls
- Detects process gaps and operational inefficiencies
- Proposes and tracks corrective measures through to implementation

Record Management and Audit Support

The Officer maintains full and organised records necessary for regulatory review, including:

- SARs, UTRs, and internal alert documentation
- Customer due diligence (CDD) and enhanced due diligence (EDD) records
- Risk evaluations, training attendance logs, and audit reports
- All policy modifications and compliance-related communications

By executing these duties, the Compliance Officer upholds the integrity of the Company's risk management and regulatory compliance systems. This role is pivotal in identifying and mitigating exposure to financial crime while ensuring the Company's operations meet the legal and supervisory obligations set by Curaçao's licensing framework for online gaming providers.

14. Senior Management

Senior management plays an essential role in maintaining the integrity and effectiveness of the Company's framework for preventing money laundering, terrorism financing, and the financing of weapons proliferation. The Board of Directors ensures that executive leadership remains fully engaged in overseeing the financial crime risk environment and in shaping the internal controls required to mitigate those risks.

The appointed AML/CTF Officer is responsible for keeping the Board informed on all key developments that may impact the Company's risk exposure or control mechanisms. This includes the delivery of an annual compliance report, which evaluates the performance of current safeguards and identifies any weaknesses or emerging threats that require senior attention.

Annual and Quarterly Oversight of Policies

Senior management holds final responsibility for confirming that all policies and related procedures addressing AML, CTF, and CPF obligations are reviewed at least once every year. This annual review process is guided by monthly risk assessments, which help identify areas where controls may be weak, operational processes inefficient, or threat patterns evolving.

When these risk assessments or updates to regulatory requirements reveal the need for policy changes, the AML/CTF Officer may recommend amendments. All proposed changes are reviewed by the Board to ensure they align with the Company's risk tolerance and legal obligations.

Oversight of Employee Training

Senior management also oversees the Company's training programs related to financial crime prevention. These programs are mandatory for all staff, particularly those in customer service, finance, and compliance departments who are most exposed to financial crime risks.

Leadership ensures that training materials remain current and relevant, incorporating updates in legislation, risk trends, and compliance standards. The objective is to strengthen employees' ability to identify suspicious behaviour, apply due diligence processes effectively, and escalate concerns in accordance with internal protocols.

Strengthening Internal Controls and Governance

Senior management is responsible for ensuring a strong internal control structure is enforced throughout the organisation. This includes setting up segregation of duties, implementing access restrictions, approving transactions based on pre-defined risk thresholds, and maintaining real-time monitoring systems to detect potential misconduct.

All decisions and actions related to internal controls are documented in detail. This practice ensures transparency, supports audit readiness, and maintains a complete record of the Company's efforts to prevent financial crime.

Independent Audits and Compliance Assurance

To confirm that the compliance framework remains effective, senior management arranges for independent audits at regular intervals, in line with Section V.5 of the Curaçao Gaming Authority's AML Guidelines. These audits assess the design and operational effectiveness of the Company's controls for managing AML, CTF, and CPF risks.

Audit results are submitted to the Board for evaluation. If deficiencies are found, the necessary corrective actions are implemented within set timeframes. This ongoing review cycle reinforces the Company's ability to detect vulnerabilities early and adapt its compliance framework as needed.

15. Employee Training and Screening

Employees are the Company's first line of defense against financial crime and regulatory breaches. To uphold this responsibility, the Company has implemented a robust employee screening and training framework designed to support a strong culture of compliance, transparency, and accountability in line with obligations related to Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF).

Employee Screening Framework

The Company enforces a structured employee screening process as outlined in Regulation V.4 of the Curaçao Gaming Authority's AML Guidelines. This framework applies during recruitment and throughout employment, particularly for individuals in roles related to compliance, finance, risk, or customer onboarding.

Pre-Employment Screening

Before hiring, all shortlisted candidates undergo a series of background checks, which include:

- Identity and work eligibility confirmation using valid government-issued documents
- Criminal background verification to detect prior financial misconduct
- Employment history and reference checks to validate reliability and experience
- Screening against international sanctions and Politically Exposed Persons (PEP) lists using certified third-party tools

Candidates who do not meet the required standards of integrity or present a compliance risk are excluded from employment consideration.

Ongoing Employee Screening

After hiring, the Company applies continuous monitoring practices to ensure employees remain suitable for their roles. These include:

- Annual re-screening for staff in sensitive or compliance-related positions
- Event-triggered checks when internal concerns arise or job responsibilities change
- Regular monitoring for changes in legal status, PEP exposure, or sanctions listings

All screening results are securely stored and managed in accordance with data protection policies, with a retention period of at least five years.

AML Training and Awareness Programme

All employees whose roles intersect with the Company's AML, CTF, or CPF obligations are required to complete mandatory training at onboarding, followed by annual refresher sessions. The training is adapted to the level of risk associated with each role and is intended to equip staff with the skills and knowledge needed to identify and manage financial crime risks effectively.

Training Topics Include:

- Curaçao's regulatory requirements and AML/CTF/CPF responsibilities
- Identification of suspicious activity and behavioral red flags such as:
 - Irregular betting or financial activity

- Use of third-party or anonymous payment methods
- Discrepancies between declared income and observed conduct
- Internal procedures for reporting Suspicious Activity Reports (SARs)
- Confidentiality during investigations and protection of sensitive client information

Employees are clearly informed that non-compliance with internal AML policies, including failure to report suspicious activity, may result in disciplinary action, including termination or legal proceedings.

Internal Escalation and Reporting

Employees are obligated to report any suspected suspicious activity to the Compliance Officer without delay using designated internal reporting channels. The Company provides clearly defined procedures and reporting tools to ensure SARs are submitted promptly, accurately, and confidentially.

Confidentiality and Data Integrity

Maintaining confidentiality is essential to the integrity of the Company's compliance programme. Employees are strictly prohibited from disclosing any information related to investigations, SARs, or unusual transactions to unauthorised parties. Any such disclosure, including tipping off, is considered a serious offence under Curaçao law and will lead to disciplinary measures.

Commitment to a Compliance-Focused Culture

Through a combination of continuous training and regular screening, the Company ensures that its staff is well-prepared to contribute to the prevention of financial crime. Employees are expected to act as active compliance partners, supporting the Company in meeting its legal responsibilities and maintaining the integrity of its operations.

16. AML Compliance Audit

The Company views internal audits as an essential component in preserving the effectiveness and integrity of its Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) systems. These audits are not treated as routine exercises, but rather as governance tools that support transparency, accountability, and continuous operational improvement. The results of all audits are formally communicated to senior management and the Board of Directors to enable prompt evaluation and corrective action where needed.

Audit Frequency and Triggers

AML compliance audits are conducted at least once per year. Additional audits may be initiated in response to regulatory updates, structural changes within the Company, or incidents that suggest weaknesses in existing controls. These audits are conducted by independent professionals—either internal or external—who are not involved in daily compliance operations but possess relevant expertise in financial crime risk management.

Scope of Audit Coverage

Each audit is tailored to assess the comprehensiveness and adequacy of the Company's compliance framework. Areas reviewed include, but are not limited to:

- **Policies and Procedures:** Evaluation of whether internal AML, CTF, and CPF policies are current, legally compliant, and consistently enforced throughout the business.
- **Risk Assessment Processes:** Review of both Business Risk Assessments (BRA) and Customer Risk Assessments (CRA), including client classification criteria and the adequacy of risk mitigation strategies.
- **Monitoring and Reporting:** Assessment of how effectively the transaction monitoring systems identify unusual or suspicious activity, and how Suspicious Activity Reports (SARs) are generated, documented, and submitted.
- **Customer Due Diligence and KYC/KYB:** Verification that client identity checks, beneficial ownership reviews, and recordkeeping practices meet internal policy standards.
- **Sanctions Controls:** Assessment of the functionality and accuracy of sanctions screening mechanisms, and their capacity to detect matches against global sanctions lists.
- **Training and Staff Vetting:** Review of the Company's employee training records, program content relevance, and pre-employment screening procedures for compliance-sensitive roles.
- **Technology and Data Integrity:** Review of the systems that support compliance processes, including access controls, data protection, and the reliability of automated scoring tools.

Reporting and Corrective Actions

Upon completion of each audit, a formal report is prepared and presented to senior management and the Board of Directors in line with Section V.7 of the Curaçao Gaming

Authority's AML Guidelines. The report outlines any observed deficiencies or control gaps, recommends specific remediation steps, and sets clear timelines for their implementation.

In cases where significant deficiencies or risks are identified, the Compliance Officer is responsible for ensuring that corrective actions are initiated without delay. Where necessary, a follow-up audit may be conducted to verify that deficiencies have been addressed and that the overall risk exposure has been brought to an acceptable level.

Recordkeeping and Regulatory Access

All documentation relating to AML compliance audits is securely maintained for a minimum of five years. These records are made available to the Curaçao Gaming Control Board or other competent authorities upon request. This approach reflects the Company's ongoing commitment to maintaining a transparent, well-governed, and legally compliant environment in relation to financial crime risk.

17. Regulatory Access and Cooperation

The Company maintains a firm commitment to transparent collaboration with the Curaçao Gaming Control Board (GCB) and any other authorised regulatory, supervisory, or law enforcement agencies. This commitment reflects the Company's governance philosophy and supports the strength of its anti-financial crime framework.

Unrestricted Access for Oversight

To support effective supervision, the Company ensures full and unrestricted access to its systems, records, personnel, and compliance infrastructure. This applies to all forms of regulatory review, including both scheduled audits and unannounced inspections conducted either remotely or on-site.

Upon request, the Company promptly provides access to:

- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) files
- Detailed transaction logs for deposits, wagers, and withdrawals
- Internal and third-party AML, CTF, and CPF risk assessments
- Compliance procedures, manuals, and operational guidelines
- Training records and compliance communications

- Internal and external Suspicious Activity Reports (SARs), including assessments and supporting documents
- System access logs and audit trails from monitoring platforms

In addition, the Company supports supervisory reviews with demonstrations of its systems, documentation walkthroughs, and other forms of practical evidence where required.

Recordkeeping and Information Security

All records necessary for regulatory review are stored securely and maintained for a minimum of five years, or longer if required under applicable law. Records are safeguarded against loss, unauthorised access, and manipulation. The Company ensures that these records are readily accessible and traceable throughout their lifecycle.

Response to Supervisory Feedback

The Company cooperates fully with feedback or formal recommendations issued by the GCB or other competent bodies. This includes:

- Implementing required remediation or policy changes within the specified deadlines
- Providing documented evidence of compliance or policy updates
- Submitting progress reports and responding to follow-up inquiries

All communication with regulatory authorities is logged and monitored to ensure proper follow-through and accountability.

Recognition of Supervisory Authority

The Company formally acknowledges the GCB's supervisory powers under Section V.6 of the CGA AML Guidelines. This includes the right to conduct examinations of the Company's AML, CTF, and CPF framework and to issue regulatory actions in the event of non-compliance or material control weaknesses. The Company accepts its responsibility to fully support such oversight and to cooperate in all examinations, whether part of a regular schedule or initiated under special circumstances.

Promoting a Culture of Compliance

The principles of regulatory cooperation are integrated into the Company's governance and compliance culture. Senior leadership actively encourages open communication with supervisory authorities and supports initiatives aimed at strengthening regulatory

relationships. By reinforcing ethical standards and operational transparency, the Company contributes to the resilience of Curaçao's gaming sector and helps to safeguard it from financial crime and regulatory abuse.

18. Internal Audit and Reporting

The Company maintains an independent internal audit mechanism that plays a critical role in evaluating and enhancing the performance, effectiveness, and integrity of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance system. Audits are conducted at least once per year, with additional reviews scheduled in response to material changes in business operations, risk exposures, or legal obligations.

Where needed, the Company may engage qualified external auditors to perform independent evaluations, particularly when technical expertise or additional objectivity is required. These external parties are selected on the basis of independence and must not be involved in day-to-day compliance tasks.

Scope of Audit Coverage

Each audit includes a detailed examination of:

- The effectiveness and compliance of AML, CTF, and CPF policies and their practical implementation.
- Transaction monitoring and sanctions screening frameworks.
- The accuracy and completeness of Suspicious Activity Reports (SARs).
- Customer onboarding, identity verification, risk rating, and due diligence procedures.
- Staff training content, delivery frequency, and effectiveness.
- The governance structure, oversight protocols, and recordkeeping practices.
- Consistency between internal control systems and the Company's stated risk appetite and regulatory obligations.

Audit Reporting and Remedial Actions

After each audit, a formal report is prepared and submitted to senior management and the Board of Directors or an assigned oversight committee. This report includes:

- A summary of the audit methodology and scope.
- Identified weaknesses or compliance gaps.
- Recommendations for improvements.
- Agreed timelines for the implementation of corrective measures.

Management is responsible for ensuring all findings are addressed within the specified timeframe. The implementation process is tracked to verify full resolution.

Compliance with Section V.5 of CGA AML Guidelines

In accordance with Section V.5 of the Curaçao Gaming Authority's AML Guidelines, the Company ensures that the internal audit function is operationally separate from the compliance department. The audit is carried out by professionals with subject matter expertise in financial crime prevention. It serves to verify both the adequacy of the policy framework and its actual execution across departments.

The audit process covers areas including:

- Business Risk Assessments (BRA) and Customer Risk Assessments (CRA).
- Execution of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD).
- Review of transaction monitoring practices and alert resolution.
- Evaluation of suspicious activity detection and STR filing processes.
- Review of screening controls for sanctions compliance.
- Assessment of the training program's structure and employee participation.

Documentation and Auditor Access

All documents related to internal audits are retained for at least five years, or longer if required by applicable law. These include audit reports, working papers, supporting documents, and tracking logs for remediation measures. The records are stored in secure environments with controlled access.

Auditors are granted unrestricted access to all systems, personnel, and documentation required to conduct their work effectively. This level of access supports comprehensive audit coverage and demonstrates compliance with regulatory expectations.

19. Record-Keeping

The Company ensures strict adherence to all legal and regulatory obligations concerning the retention and management of records, maintaining a complete, traceable, and auditable trail for inspection by competent authorities when required. In accordance with applicable data protection laws, all records are securely preserved in digital format for a minimum period of five (5) years from the commencement of any business, commercial, or professional relationship with a customer, employee, or third party.

To support ongoing compliance with Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) requirements, the Company has implemented formal procedures for storing and protecting all key documentation, including but not limited to:

- Verified identification data and customer due diligence (CDD/EDD) records
- Full transaction histories and related communications
- Internal Suspicious Activity Reports (SARs) and corresponding assessments
- AML/CTF/CPF training records specific to employees' roles and responsibilities
- Internal and external audit reports relevant to the compliance framework

All records are stored in encrypted systems with robust access controls. Access to these systems is strictly limited to authorised personnel, and all access attempts are logged and subject to periodic review.

To ensure continued integrity and availability of records, the Company conducts regular audits of its record-keeping infrastructure. These reviews verify that data is complete, accurate, securely maintained, and readily accessible for regulatory inspection, audit, or investigation.

20. Appendices

Appendix 1: Customer Risk Calculator

HOW TO USE THIS?
 1. Only yellow and blue fields have to be filled.
 2. Comment section is available, however, it is not necessary for calculation of risk level.
 3. Majority of questions has dropdown list or checkbox. Correct answer(-s) should be selected.

NEW total score:	0.00
NEW risk level:	Low
Onboarding specialist:	
Last update date:	

Category	Score
low	0-1.8
medium	1.9-2.5
high	2.6 or more
unacceptable	At least 4 unacceptable

Question	Risk score	Risk level	Additional comments
Customer's Age			
Customer's Citizenship			
Customer's Second Citizenship			
Customer's Country of Birth			
Customer's Country of Residence			
Does Customer have the status of PEP/IRCA (Politically Exposed Person/Relative and Close Associate)?			
ACCOUNT PROFILE			
Purpose of account registration?			
FUND SOURCE AND INCOME STATUS			
Source of funds	average		
Source of wealth	average		
INTENDED ACCOUNT ACTIVITY (DEPOSITS)			
Average frequency of transactions			
Expected total value of transactions per period (NAP)			
Types of incoming payments	average		
INTENDED ACCOUNT ACTIVITY (OUTGOING PAYMENTS)			
Average frequency of transactions			
Expected total value of transactions per period (NAP)			
Types of outgoing payments	average		
Reasons for outgoing payments	average		
GAMING BEHAVIOUR			
Please indicate services of interest	average		

Risk Category:	To be:	Sum:	Weight:
Client	20%	0	
Geography	20%	0	
Products and Services	20%	0	
Transactions	20%	0	
Channels	15%	0	
Other	5%	0	
		0	

CONFIRMATIONS			
Channels	average		
Adverse media level			
Manual risk level adjustment based on the expert judgement (x0.5):			Comment regarding manual risk adjustment: Summary of the applicant:

Appendix 2: Employee Onboarding & Screening Form

Employee Screening Program

This Employee Screening Program outlines the mandatory procedures for evaluating and continuously monitoring all individuals employed or otherwise engaged by the Company. It has been designed in accordance with Regulation V.4 of the Curaçao Gaming Authority (CGA) AML Guidelines, which require effective screening before employment and throughout the duration of service.

A dedicated **Employee Screening Checklist** must be completed for every case to confirm that all prescribed steps have been followed.

Scope of Application

This program applies to the following categories of individuals:

- All employees, including permanent, temporary, and contract-based personnel
- Members of senior management, the Compliance Officer, and any staff involved in AML, CTF, or CPF functions
- Individuals engaged through outsourced or third-party arrangements who carry out regulated or sensitive duties

No person may be assigned to a sensitive or regulated role until all screening requirements have been fulfilled.

Screening Requirements

The Company ensures that personnel are appropriately qualified, trustworthy, and suitable for their assigned roles. Screening measures vary depending on the sensitivity of the role and are fully documented.

The screening process includes:

- Pre-employment checks
- Fit-and-proper assessments for designated positions
- Ongoing employee monitoring
- Completion of the Employee Screening Checklist

1. Pre-employment Checks

Before hiring a candidate, the Human Resources department, in coordination with Compliance, conducts the following steps:

- **Criminal record check:** To detect any past convictions, particularly related to financial crime, fraud, or misconduct
- **Verification of identity:** Using valid government-issued identification, reviewed for accuracy and authenticity
- **Verification of academic and professional qualifications:** Independent confirmation of submitted credentials
- **Employment history review:** Verification of prior roles and assessment of performance and conduct
- **Reference checks:** At least two professional references must be collected. Any adverse findings are escalated to the Compliance team

Employment offers are not finalized until all checks are completed and the checklist has been signed.

2. Fit-and-Proper Assessment

For high-level or sensitive roles, a formal fit-and-proper assessment is conducted. This includes:

- **Integrity and reputation:** No history of regulatory sanctions, criminal convictions, or disciplinary actions
- **Professional competence:** Verified knowledge, expertise, and experience, particularly in AML or regulated roles
- **Financial reliability:** A background check for bankruptcy or insolvency, where legally permitted

- **Independence and impartiality:** Evaluation of conflicts of interest

The completed assessment is reviewed and approved by the Compliance Department and retained with other screening documentation.

3. Ongoing Monitoring of Employees

Monitoring continues after employment through the following measures:

- **Annual rescreening** for personnel in high-risk or compliance-related roles
- **Event-based rescreening** in cases such as internal investigations, job changes, or new regulatory guidance
- **Conduct-based reporting**, requiring managers or Compliance to escalate concerns about integrity or fitness

All activities are recorded in the Employee Screening Checklist.

4. Documentation and Retention

The Company maintains comprehensive records of all screening activities, including:

- Background check results
- Identification and qualification documents
- Fit-and-proper assessments
- Screening checklists
- Internal approvals, concerns, and corrective actions

All documents are securely stored and retained for at least five years, or longer where required by law. They are made available to competent authorities upon request and maintained in compliance with data protection regulations.

Roles and Responsibilities

- **Human Resources:** Oversees pre-employment screening, ensures documentation is completed and archived, and refers any issues to Compliance
- **Compliance Officer:** Leads screening for regulated roles, approves appointments to sensitive positions, and ensures full compliance with Regulation

- **Senior Management:** Provides oversight and resources, reviews escalations, and receives regular updates on screening practices

Compliance and Enforcement

Failure to comply with this screening program, including incomplete documentation or missing assessments, may result in disciplinary action or dismissal.

The Company confirms that this program is reviewed annually to ensure alignment with Regulation V.4 of the CGA AML Guidelines and with evolving legal and regulatory requirements.

New Employee Checklist

Employee Name and Position:

Start Date:

The following documents must be collected and verified before the employee's official start date. Mark each item as received and verified:

- National identity card or passport
- Valid work permit (if applicable)
- Proof of residence
- Certificate of no criminal record
- Non-bankruptcy confirmation
- Reference letter from previous employer
- Professional licenses or certificates (if required)
- Curriculum Vitae (CV)
- Good repute questionnaire
- Diploma of higher education
- Signed acknowledgement of AML and IOM policies
- Signed privacy notice
- Induction and initial training form
- Signed employment agreement

Reviewed by HR:

Date: