

LOTOSTORM B.V. (163910)

Abraham Mendez Chumaceiro Boulevard 03, Curacao



AML/CTF/CPF Policy

Version 3

12/12/2025

Approved by the Board of Directors:



Responsible Compliance Officer:

Semen Klyuchyk
compliance@lotostorm.com

Version 1: 27/02/2025

Version 2: 25/03/2025

Version 3: 12/12/2025

Next Review: December 2026

Table of Contents

1. Definitions & Abbreviations	3
2. Policy Statement	7
3. iGaming Landscape	8
4. Money Laundering, Terrorism Financing & Proliferation Financing	9
5. Integration of the National Risk Assessment	15
5.1. Customer Risk Assessment	18
5.2. Ongoing Monitoring	21
6. Risk-Based Approach	23
7. Customer Due Diligence & Enhanced Due Diligence	27
8. Customer Acceptance Policy	32
9. Transaction Monitoring	53
10. Politically Exposed Persons	55
11. Sanctions Policy	57
12. Suspicious & Unusual Activity & Transaction Reporting	65
12.1. Suspicious & Unusual Activity	67
12.2. Suspicious & Unusual Transactions	68
12.3. Timely Reporting	69
12.4. Confidentiality & Commitment to the Strong Reporting Culture	69
13. Compliance Officer	70
14. Senior Management	72
15. Employee Training & Screening	73
16. AML Compliance Audit	76
17. Regulatory Access & Cooperation	77
18. Internal Audit & Reporting	79
19. Record-Keeping	81
20. Appendices	83
Appendix 1: Client Risk Calculator	83
Appendix 2: Employee Onboarding & Screening Form	84

1. Definitions and Abbreviations

AML – Anti-Money Laundering, a framework of regulations and policies designed to prevent financial crimes.

BoD – Board of Directors of the Company, responsible for governance and oversight of compliance measures.

CFATF – The Caribbean Financial Action Task Force, a regional body of 24 Caribbean, Central, and South American states focused on combating money laundering and terrorist financing.

Compliance Officer – A senior management member responsible for detecting and preventing money laundering, terrorist financing, and proliferation financing risks, operating independently from gaming operations.

CTF – Counter-Terrorism Financing, the process of identifying and preventing the funding of terrorist activities.

CPF – Counter-Proliferation Financing, measures aimed at preventing financial support for the spread of weapons of mass destruction.

CDD – Customer Due Diligence, procedures used to verify customer identity and assess financial risk.

EDD – Enhanced Due Diligence, additional verification and risk assessment measures applied to high-risk individuals or entities.

FIU – Financial Intelligence Unit of Curaçao, as defined in Article 2 of the NORUT, responsible for analyzing and processing reports on suspicious financial transactions.

KYB – Know Your Business, a process for verifying and understanding business entities to ensure compliance.

KYC – Know Your Customer, policies and procedures to verify the identity of customers and monitor their financial activities.

SOF/SOW – Source of Funds/Source of Wealth, verification of the origin of financial assets to prevent money laundering.

UBO – Ultimate Beneficial Owner, the individual who ultimately owns or controls an account or transaction.

SAR/STR – Suspicious Activity Report/Suspicious Transaction Report, official reports submitted to regulatory authorities when financial transactions appear suspicious.

PEP – Politically Exposed Person, an individual with a high-profile political or public function, requiring additional scrutiny due to increased risk of financial crimes.

UN – United Nations, an international organization that develops and enforces measures against money laundering and terrorist financing.

EU – European Union, a political and economic union with AML/CTF directives applicable to its member states.

UK – United Kingdom, which enforces its own AML/CTF regulations and financial crime compliance measures.

US – United States, with financial crime regulations overseen by agencies such as OFAC and the Financial Crimes Enforcement Network (FinCEN).

OFAC – Office of Foreign Assets Control, a U.S. Treasury Department agency responsible for enforcing economic sanctions.

FATF – Financial Action Task Force, an international organization that establishes global AML and CTF standards and maintains lists of high-risk jurisdictions.

NOOGH – National Ordinance on Offshore Games of Hazard, Curaçao legislation governing offshore gaming activities.

Money Laundering

Money laundering is the process of disguising illicitly obtained funds to make them appear legitimate. It typically involves three stages:

1. Placement – Introducing illicit funds into the financial system.
2. Layering – Conducting complex transactions to obscure the origin of the funds.
3. Integration – Reintroducing laundered money into the legitimate economy.

AML Policy

An AML policy is a formal framework of internal policies, procedures, and controls designed to prevent money laundering and terrorist financing. It is managed by the AML compliance team, led by the Money Laundering Reporting Officer (MLRO), who is responsible for overseeing AML training and conducting independent audits.

Anti-Money Laundering and Counter-Financing of Terrorism Program (AML/CTF/CPF Program)

A structured program developed to prevent financial crime, consisting of internal policies, risk assessments, monitoring systems, and reporting mechanisms. The MLRO

oversees the program, ensuring compliance with legal requirements and regulatory best practices.

Money Laundering Reporting Officer (MLRO)

The MLRO is the designated officer responsible for implementing AML policies, monitoring financial transactions, filing Suspicious Transaction Reports (STRs), and ensuring regulatory compliance.

Alerts and Transaction Monitoring

An alert is a notification triggered by predefined red flags, requiring further investigation. Transaction monitoring systems detect potential financial crime by analyzing patterns and identifying anomalies.

Regulatory Bodies and Supervisory Authorities

- Curaçao Gaming Control Board (GCB): The primary AML/CTF supervisory authority for the gaming sector.
- Financial Intelligence Unit (FIU): The national agency responsible for receiving, analyzing, and escalating reports on suspicious transactions.
- Financial Action Task Force (FATF): An international body that establishes AML/CTF guidelines and maintains blacklists and greylists for non-compliant countries.

Know Your Customer (KYC) and Due Diligence Measures

- KYC: Policies and procedures for verifying a customer's identity and assessing their transaction patterns.
- Customer Due Diligence (CDD): A process that involves verifying identities, assessing risk, and monitoring transactions for suspicious activity.
- Enhanced Due Diligence (EDD): Additional verification steps for high-risk customers, including obtaining information on source of wealth and business activities.

Sanctions Compliance and Screening

- Beneficial Owner: The person who ultimately controls an account or transaction.
- Sanctions: Restrictions imposed on countries, individuals, or entities due to security concerns, including trade bans and asset freezes.
- Automated Screening Tools (AST): Software used to screen customers against sanctions lists and flag restricted entities.
- Blacklist: A list of entities, individuals, or locations subject to financial restrictions.
- Comprehensive Sanctions: Measures prohibiting all financial dealings with a sanctioned country, except in rare exceptions.

Risk Management and Financial Crime Prevention

- Risk-Based Approach (RBA): A methodology for assessing and managing financial crime risks based on transaction types, customers, and jurisdictions.
- Risk Appetite: The level of risk an institution is willing to accept within its operations.
- High-Risk Third Country: A country designated by FATF or the European Commission as posing an elevated AML/CFT risk.
- Economic Sanctions: Trade or financial restrictions imposed by governments to influence political or economic behavior.

Record-Keeping and Reporting Obligations

- Suspicious Transaction Report (STR): A formal report submitted to the FIU when a transaction raises AML/CTF concerns.
- Unusual Transaction: Any transaction that deviates from expected patterns, potentially indicating illicit activity.
- Audit Logs: Records maintained for at least five years, documenting AML compliance efforts.
- First Line of Defense: Employees responsible for collecting customer information and identifying suspicious activity during onboarding.

Money Laundering Techniques and Prevention Measures

- Structuring: The process of making multiple smaller transactions to evade reporting thresholds.
- Layering: The act of moving illicit funds through multiple transactions to obscure their origin.
- Integration: The final stage of money laundering, where funds appear fully legitimate.
- Sanctions Evasion: Attempts to conceal transactions involving sanctioned entities to bypass financial restrictions.

International Cooperation and AML Standards

- Office of Foreign Assets Control (OFAC): A U.S. agency enforcing economic sanctions.
- Egmont Group of FIUs: A global network of Financial Intelligence Units that facilitates AML/CTF information exchange.
- The Wolfsberg Group: An association of global banks that develops best practices for private banking AML compliance.

2. Policy Statement

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

LOTOSTORM B.V. (163910) has developed an Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing Policy (AML/CTF/CPF Policy) to actively prevent financial crimes such as money laundering and terrorism financing. This policy is structured to align with both domestic and international AML/CTF/CPF standards and ensures strict adherence to relevant regulatory requirements. It establishes a comprehensive risk management framework covering various aspects, including customer engagement, product and service offerings, payment channels, geographic areas of operation, and service delivery methods.

The Board of Directors (BoD) of LOTOSTORM B.V. holds the responsibility for approving, enforcing, and overseeing the AML/CTF/CPF Policy. This policy undergoes an annual review and may be revised as necessary to incorporate significant regulatory or operational updates. Additionally, a designated officer may recommend immediate amendments in response to findings from internal and external AML audits, taking into account potential risks and implications.

This AML/CTF/CPF Policy is structured in accordance with key international and Curaçao regulatory frameworks. LOTOSTORM B.V. strictly adheres to the Regulations for Combating Money Laundering, Terrorism Financing, and the Proliferation of Weapons of Mass Destruction (ML/FT/FP) as these regulations are a fundamental component of iGaming licensing requirements within the Curaçao jurisdiction and are at the core of the Company’s operations:

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

Through these regulations, the Curaçao Gaming Control Board (GCB) provides a structured framework to guide casinos and gambling operators in ensuring compliance with laws and decrees related to money laundering, terrorism financing, and proliferation financing. This framework serves as the core of LOTOSTORM B.V. development and implementation of internal policies and procedures to mitigate financial crime risks.

The key regulatory provisions LOTOSTORM B.V. complies with include, but are not limited to:

- The National Ordinance on Identification of Clients When Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree (dated November 11, 2015) outlining indicators under Article 10 of the National Ordinance on Reporting Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree on the Enforcement of the Kingdom Sanction Law (N.G. 2017, no. 2);
- National Decree (dated July 10, 2015) implementing UN Security Council Resolutions regarding Al-Qaeda, the Taliban, ISIL, ANF, and other designated individuals and organizations (N.G. 2015, no. 29);
- National Decree (dated July 10, 2015) implementing Article 2 of the Sanctions National Ordinance concerning Libya (Sanctions Ordinance Libya) (N.G. 2015, no. 28);
- National Decree (dated July 10, 2015) implementing Article 2 of the Sanctions National Ordinance concerning UN Security Council Resolutions 1695 (2006), 1718 (2006), 2087 (2013), and 2094 (2013) (Sanctions National Ordinance 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 and regulations, along with any supplementary measures established under the NOIS, NORUT, the Sanctions National Ordinance, and the Kingdom Sanction Law, form the primary legal framework that governs the Curaçao gaming industry in its efforts to prevent money laundering, terrorism financing, and the proliferation of weapons of mass destruction.

In addition to local regulations, this policy incorporates global best practices and follows guidelines from recognized international organizations, including but not limited to the Financial Action Task Force (FATF) Recommendations, the European Union's 4th, 5th, and 6th Anti-Money Laundering Directives (AMLDs), and the Wolfsberg Principles.

Ultimately, the AML/CTF/CPF Policy of LOTOSTORM B.V. (163910) is designed to meet the compliance requirements set by Curaçao's AML/CTF/CPF supervisory authority, the Curaçao Gaming Control Board. All company directors, officers, employees, and third-party auditors engaged in compliance assessments are required to adhere to and uphold the principles outlined in this policy.

3. iGaming Landscape

LOTOSTORM B.V. (163910) (hereinafter, the "Company") is a legally registered entity in Curaçao that owns and operates the website <https://clickpari.com>. The company holds

an online gaming license issued by the Curaçao Gaming Control Board, specifically OGL/2024/303/0300, and complies with all licensing regulations and regional restrictions established by the Curaçao regulatory authorities. These regulations strictly prohibit remote gaming licensees from providing services in certain 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, the company operates only in legally authorized markets and refrains from targeting customers in regions where online gambling is prohibited.

Like other e-gaming and betting operators, LOTOSTORM B.V. is exposed to various money laundering risks, including identity theft, fraudulent activities, structuring, layering, and the potential for collusion between employees, customers, or third-party payment providers to bypass internal security controls.

4. Money Laundering, Terrorism Financing & Proliferation Financing

Money laundering is a key component of financially motivated crime, often involving cross-border operations. It is linked to various illegal activities, including tax evasion, fraud, corruption, sanctions violations, drug trafficking, illegal arms trade, extortion, and kidnapping. The primary objective of money laundering is to conceal the illicit origins of proceeds derived from criminal activities by obscuring their source, identity, and final destination.

The Three Stages of Money Laundering

1. Placement – This is the initial stage, where illicit funds are introduced into the financial system. This is done through bank deposits, purchasing high-value assets, or conducting various financial transactions. The goal at this phase is to start integrating illegal funds into the legitimate economy.
2. Layering – In this phase, the money is moved through multiple complex transactions to further obscure its origins. Techniques include transferring funds across numerous accounts, converting funds into different currencies, or investing in various financial instruments. This process is intended to eliminate traceability, making it difficult to link the funds back to criminal activities.
3. Integration – The final stage involves reintroducing the laundered funds into the legal economy. This may be done through purchasing luxury assets, investing in cash-intensive businesses, or engaging in other seemingly legitimate financial transactions. At this point, the money appears clean, making it significantly harder to trace back to its illicit source.

Money laundering can occur at different stages of financial transactions, and online gambling platforms are particularly vulnerable to being exploited for this purpose. This underscores the importance of preventing anonymous transactions and identifying suspicious activities.

Terrorist Financing and Its Connection to Money Laundering

Terrorist financing refers to the movement of funds used to support terrorist activities. Unlike money laundering, these funds may originate from legitimate sources but are transferred through financial systems in a way that resembles laundering techniques. Prepaid cards, for example, are frequently used to fund terrorist operations by purchasing materials for attacks. To combat such risks, LOTOSTORM B.V. (163910) ensures that employees receive ongoing training on emerging trends and evolving threats related to terrorist financing.

Risk Management and Compliance Measures

To mitigate money laundering risks, LOTOSTORM B.V. (163910) adopts a proactive approach by detecting, assessing, and addressing potential threats. Key compliance strategies include:

- **Fraud and Identity Verification** – Implementing customer due diligence (CDD) processes, including document verification, age validation, and location checks.
- **Monitoring Multiple Accounts and High-Value Transactions** – Identifying unusual account activity, including the use of multiple accounts or frequent large transactions.
- **Detecting Illicit Fund Deposits** – Screening for suspicious deposits originating from illicit activities and preventing the platform from being used as a temporary holding space for such funds.
- **Player-to-Player Transfers** – Monitoring for potential misuse of the platform to transfer illicit funds between users or enable fraudulent cash-out activities.

This list is not exhaustive, as new risks may emerge over time. To ensure robust compliance, LOTOSTORM B.V. (163910) conducts regular risk assessments tailored to evolving threats and provides ongoing training to employees to reinforce its Anti-Money Laundering (AML) compliance framework.

Terrorism Financing

Terrorist financing refers to the funding of terrorist activities, utilizing both legitimate and illicit financial sources. These funds are critical for carrying out operations ranging from small-scale activities to large-scale attacks.

Sources of Terrorist Financing

The sources of financing can be broadly divided into legal and illegal categories:

- **Legal Sources** – Terrorists may exploit legitimate businesses, charitable donations, and legal financial transactions to funnel funds. In some cases, charitable organizations and commercial enterprises are misused as conduits to disguise and redirect money.

- **Illegal Sources** – Criminal activities such as fraud, smuggling, drug trafficking, extortion, and money laundering are commonly used to generate funds while obscuring their origins.

Methods of Fund Transfers

Terrorist financing networks use various channels to move funds:

- **Formal Financial Channels** – Traditional banking systems and financial institutions are sometimes exploited through sophisticated techniques like layering and structuring, which help avoid detection by breaking transactions into smaller, less suspicious amounts.
- **Informal Transfer Systems** – Alternative financial networks such as the hawala system operate outside regulated financial institutions, making it difficult for authorities to trace transactions.

Indicators of Terrorist Financing

Certain transaction patterns may indicate potential terrorist financing, including:

- **Unusual financial activity** that deviates from typical business or personal behavior.
- **Frequent or high-value transactions** involving high-risk regions known for terrorist activities.
- **Transactions associated with individuals or entities linked to terrorism**, including those flagged on international watchlists.
- **Large cash deposits, high-risk industry transactions, or financial activities** that seem structured to avoid scrutiny.

Regulatory Compliance and Countermeasures

To combat terrorist financing, LOTOSTORM B.V. (163910) implements a comprehensive AML compliance program that includes:

- **Customer Due Diligence (CDD)** – Verifying customer identities, sources of funds, and potential risks.
- **Transaction Monitoring** – Analyzing financial transactions for suspicious patterns.
- **Reporting Suspicious Activities** – Notifying relevant authorities of any potential terrorist financing indicators.

The company also adheres to multiple sanctions lists and regulatory directives, including:

- **Sanctions National Ordinance (SNO, N.G. 2014, no. 55)**
- **Kingdom Sanction Act (N.G. 2016, no. 54)**
- **Curaçao Gaming Control Board (GCB) regulatory announcements**
- **Office of Foreign Assets Control (OFAC) watchlists**
- **United Nations Security Council (UNSC) sanctions lists**

- European Union (EU) anti-terrorism financial regulations
- U.S. List of Foreign Terrorist Organizations

These sanctions and regulatory measures help ensure that the company does not inadvertently facilitate financial transactions that may support terrorism.

Global Framework for Counter-Terrorism Financing

- Financial Action Task Force (FATF) – Establishes international standards for detecting and reporting suspicious financial activity related to money laundering and terrorist financing.
- Office of Foreign Assets Control (OFAC) – Enforces U.S. economic sanctions and maintains the Specially Designated Nationals (SDN) list, which includes individuals and entities associated with terrorism.
- European Union (EU) – Enforces regulatory frameworks designed to prevent the exploitation of financial systems for terrorist activities, requiring member states to implement strong AML measures.
- United Nations (UN) – Imposes international sanctions and maintains watchlists of individuals and organizations involved in terrorism, supporting global efforts to restrict financial access for terrorist groups.

By implementing strict compliance policies and adhering to international regulatory frameworks, LOTOSTORM B.V. (163910) strengthens its ability to detect, prevent, and report terrorist financing activities, ensuring a secure and legally compliant operational environment.

Proliferation Financing

Proliferation financing refers to the provision of financial resources or support for the development, acquisition, and distribution of weapons of mass destruction (WMDs), including their delivery systems. This type of financing is a significant threat to global security and is strictly prohibited under international and Curaçao regulations. As an operator in the iGaming sector, the Company. is committed to addressing the risks associated with proliferation financing as part of its broader Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework.

Compliance with Curaçao iGaming Regulations:

The Curaçao Gaming Control Board (GCB) has implemented enhanced compliance requirements to address proliferation financing risks, reflecting the evolving global standards. These requirements obligate all licensed operators, including the Company., to identify, mitigate, and report potential risks associated with proliferation financing. Key elements include:

1. Risk Assessment

The Company. conducts regular risk assessments to identify vulnerabilities

specific to proliferation financing within its operations. These assessments consider factors such as:

- The use of the platform by customers from high-risk jurisdictions with weak proliferation controls.
- Transactions involving goods, services, or entities linked to WMD proliferation networks.
- Patterns of financial activity consistent with known methods of proliferation financing.

2. Enhanced Customer Due Diligence (CDD)

The Company. implements enhanced CDD measures to verify the identity of customers, particularly those from high-risk jurisdictions. This includes:

- Screening customers against international sanctions lists, including those maintained by the United Nations Security Council, the Financial Action Task Force (FATF), and the European Union.
- Investigating the purpose and intended nature of transactions that deviate from standard patterns.
- Monitoring for customers with affiliations to entities flagged for involvement in proliferation-related activities.

3. Transaction Monitoring and Reporting

Advanced transaction monitoring systems are employed to detect unusual or suspicious activity that may indicate proliferation financing. These systems analyze transaction patterns, flag high-risk transactions, and ensure that suspicious activity reports (SARs) are promptly filed with relevant authorities, including the Curaçao Financial Intelligence Unit (FIU).

4. Sanctions Screening and Compliance

The Company. strictly adheres to the sanctions and compliance requirements established by Curaçao and international regulatory bodies. This includes:

- Prohibiting transactions involving individuals, entities, or jurisdictions subject to WMD-related sanctions.
- Screening all financial transactions and business relationships against updated sanctions lists, including the Kingdom Sanction Act and United Nations Security Council Resolutions.
- Maintaining detailed records of sanctions screening and reporting results for audit and regulatory review.

5. Training and Awareness

Employees at the Company receive specialized training on proliferation financing risks, including how to identify red flags and respond appropriately. This training ensures that staff remain vigilant and equipped to comply with Curaçao's evolving regulatory landscape.

6. Collaboration with Authorities

The Company. works closely with the Curaçao Gaming Control Board, Financial Intelligence Unit (FIU), and other relevant authorities to strengthen compliance. The company ensures full cooperation in investigations, provides timely reporting, and participates in initiatives aimed at combating proliferation financing in the iGaming sector.

Commitment to Global Security:

The Company recognizes the critical importance of preventing its platform from being misused to facilitate proliferation financing. By adhering to Curaçao's new iGaming compliance requirements and international standards, the company reinforces its commitment to maintaining a secure, transparent, and compliant gaming environment. These efforts contribute to global initiatives aimed at safeguarding financial systems from exploitation by those seeking to develop or distribute weapons of mass destruction.

5. Integration of the National Risk Assessment

Overview

The Company maintains a comprehensive and flexible compliance program designed to mitigate the risks of money laundering, terrorist financing, and the financing of weapons of mass destruction. This framework is intended to protect all aspects of the Company's operations, including its online gaming services, financial transactions, and supporting infrastructure.

The compliance program is implemented in accordance with Curaçao's legislative and regulatory standards, particularly those issued by the Curaçao Gaming Control Board (GCB). It also aligns with international best practices as established by the Financial Action Task Force (FATF) and the Caribbean FATF (CFATF). All stakeholders, including employees, senior management, partners, and third-party service providers, are expected to operate in full compliance with these standards.

Governance and Oversight

The Board of Directors has overall responsibility for the design, approval, and strategic oversight of the Company's AML, CTF, and CPF compliance framework. It ensures the allocation of adequate financial, human, and technical resources to address the unique risks inherent in the remote gaming sector.

Senior Management is responsible for translating these strategic objectives into operational practice. This includes guaranteeing that the Compliance Officer has unrestricted access to systems, tools, personnel, and all relevant information necessary to carry out compliance responsibilities effectively.

Role of the Compliance Officer and Application of the NRA

The Compliance Officer is charged with managing the daily implementation of the Company's compliance program. This includes oversight of customer due diligence

(CDD and EDD), monitoring of transactions, execution of internal investigations, and submission of reports to the Financial Intelligence Unit (FIU) of Curaçao.

In accordance with AML Regulation III.1, the Compliance Officer ensures that the Company's internal controls are updated as needed to respond to changes in regulatory requirements and evolving financial crime threats.

The Company integrates findings from the latest National Risk Assessment (NRA) issued by Curaçao's competent authorities. These findings are used to enhance internal risk assessments, reassess customer profiles, evaluate geographic exposure, and strengthen controls in areas identified as vulnerable to abuse.

Implementation of NRA Findings

Insights from the NRA are incorporated into the Company's enterprise-level risk assessment and applied throughout the operational environment. Specific actions taken by the Compliance Officer based on NRA findings include:

- Enhancing onboarding and identity verification protocols
- Calibrating transaction monitoring thresholds to reflect new risk typologies
- Applying stricter controls for customer segments, jurisdictions, or payment channels flagged as high risk
- Introducing targeted surveillance measures in response to newly emerging threats

Whenever new or emerging risks are identified, the Compliance Officer assesses the sufficiency of current controls and implements enhancements as necessary.

Risk-Based Due Diligence

The Company applies Know Your Customer (KYC) procedures proportionate to the risk level of each customer. These procedures are performed before processing withdrawals and whenever customer behavior exceeds predefined activity thresholds.

Standard due diligence includes verification of identity, confirmation of age and address, and validation of payment methods. Where elevated risks are detected, especially risks identified in the NRA, Enhanced Due Diligence (EDD) measures are applied. These may include:

- Verified documentation of the customer's source of funds and wealth
- Expanded screening using media and regulatory sources

- Review and approval by senior compliance or management personnel

EDD is mandatory for high-risk customers, such as politically exposed persons (PEPs), players from high-risk jurisdictions, high-value customers, and those exhibiting suspicious behavior.

Monitoring and Escalation

The Company employs a dual-layered monitoring system that combines automated transaction analysis with manual review by trained compliance personnel. This system is designed to detect red flags such as:

- Irregular or unexplained deposit and withdrawal patterns
- Betting behavior that appears abnormal or inconsistent
- Use of VPNs or proxy servers to mask customer location
- Repeated abuse of promotional incentives or frequent changes to account details

All alerts generated by the monitoring system are escalated to the Compliance Officer for review. If activity is assessed as suspicious, a report is filed with the FIU via the goAML platform, in line with AML Regulation IV.1 and the requirements of the National Ordinance on the Reporting of Unusual Transactions (NORUT).

Employees are required to escalate any suspicious or unusual activity immediately. The Company enforces strict confidentiality and prohibits tipping off or unauthorized disclosure of compliance investigations. Any breach is treated as a serious disciplinary violation.

Record-Keeping and Training

The Company maintains all compliance-related records for at least five years. This includes:

- KYC documentation
- Transaction records and monitoring reports
- Internal alerts and escalation logs
- Internal and external audit findings
- Documentation relating to the National Risk Assessment

All employees performing compliance duties receive structured training on AML, CTF, and CPF obligations. Training modules include guidance on interpreting NRA results and understanding the national financial crime landscape. Training is provided at least annually and is updated as required following regulatory changes or the identification of new risks.

The Compliance Officer is responsible for ensuring that the compliance program is reviewed on an annual basis and that any updates are implemented in line with NRA findings and GCB guidance.

5.1. Customer Risk Assessment

Risk-Based Evaluation Approach

The Company applies a structured, risk-based methodology to assess the potential exposure of each customer to money laundering (ML), terrorist financing (TF), and proliferation financing (PF). This assessment is conducted through a formalized client risk scoring model that evaluates various indicators, including transaction patterns, geographical risk connections, and other behavioral and contextual factors. The purpose of this model is to ensure that the level of due diligence and monitoring applied corresponds appropriately to the risk profile assigned to each customer.

Risk Scoring Methodology

Each risk variable within the model is assigned a numerical value, and the aggregated score determines the customer's overall risk classification. This classification informs the type and depth of due diligence required and dictates the level of internal approval necessary for both onboarding and ongoing relationship management.

Risk Category	Score Range	Due Diligence Level	Approval Required
Low Risk	0 to 2	Standard Due Diligence	Client Services or Compliance Officer
Medium Risk	2 to 4	Standard Due Diligence	Client Services or Compliance Officer
High Risk	4 and above	Enhanced Due Diligence	Compliance Officer with annual review
Unacceptable Risk	Trigger-based	Relationship Rejected	Automatically Declined

Customers within the low and medium risk tiers are subject to standard due diligence measures, which include identity verification and periodic account review. Those classified as high risk must undergo enhanced due diligence (EDD), which requires the submission of additional supporting documents, formal approval by the Compliance Officer, and annual review of the relationship.

Clients identified as posing an unacceptable level of risk are denied access to the platform. This includes persons or entities appearing on sanctions lists or exhibiting severe red flags that exceed the Company's documented risk tolerance.

The risk scoring model is subject to regular updates to ensure continued relevance in light of new regulatory developments, emerging criminal typologies, and changes in industry conditions.

Screening and Risk Treatment

All customers, regardless of their risk classification, are screened at onboarding and throughout the business relationship. The screening process includes checks for:

- Sanctioned status under domestic or international frameworks
- Identification as a Politically Exposed Person (PEP) or close associate
- Exposure to adverse media or negative regulatory findings

The screening system operates in real time and is supported by a reliable third-party screening service. Risk classification results are reviewed periodically and adjusted based on new information or changes in behavior.

Treatment by Risk Category

Low-Risk Customers

Customers classified as low risk are considered to present minimal exposure to ML, TF, or PF. Nevertheless, simplified due diligence is not applied. All low-risk customers are subject to full standard due diligence measures, in line with Curaçao AML regulations and the Company's internal policies.

Medium-Risk Customers

Medium-risk customers exhibit moderate risk indicators that warrant closer scrutiny. These clients must fulfill all Know Your Customer (KYC) obligations and are subject to periodic reviews to confirm that their risk profile remains accurate and consistent with observed behavior.

High-Risk Customers

Customers classified as high risk are subject to enhanced onboarding procedures and ongoing monitoring. Approval from the Compliance Officer is mandatory prior to establishing or continuing a relationship. Risk factors that may trigger a high-risk classification include:

- Use of complex ownership or legal structures
- Transactions that do not align with declared source of funds or profile
- Links to jurisdictions categorized as high risk or under sanctions
- Identification as a PEP or close associate
- Negative findings in media reports or from regulators
- Provision of falsified or unverifiable documents
- Lack of transparent legal or economic rationale for transactions
- Intermediation or use of the account by third parties
- Cumulative deposits exceeding designated high-risk thresholds

Unacceptable Client Profiles

The Company maintains a defined risk appetite and will not establish or maintain relationships with individuals or entities that:

- Are listed on domestic or international sanctions registers
- Are reasonably suspected of involvement in money laundering, terrorism financing, or proliferation financing
- Are below the minimum legal age or fail to meet age verification requirements
- Are unable or unwilling to verify the source of funds or wealth
- Display abusive or manipulative behavior within the gaming environment

Any customer who falls within the unacceptable risk category is automatically rejected. All decisions regarding onboarding, risk classification, rejection, or escalation are thoroughly documented and retained for future reference.

Ongoing Review and Enhancement

The Company continually reviews and refines its customer risk assessment framework. Updates are informed by internal findings, evolving regulatory expectations, and sector-specific trends. This ensures that the risk assessment methodology remains both effective and compliant with the latest standards applicable to the online gaming and financial services environment.

5.2. Ongoing Monitoring

The Company maintains a continuous customer monitoring program that reflects its risk-based compliance strategy and supports its obligations under Curaçao's Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) regulations. This monitoring ensures that customer information remains up to date, risk profiles are accurate, and that suspicious activity is detected and addressed in a timely manner.

Continuous Screening Activities

The Compliance Department conducts regular screenings of all active customers using external databases. These include international and domestic sanctions lists, registers of Politically Exposed Persons (PEPs), and adverse media sources. When a match is confirmed, the case is escalated for further review. If the new information affects the customer's risk classification, a full reassessment is performed without delay.

Event-Driven Reassessments

The Company performs event-based reviews whenever specific risk triggers arise. These reviews may result in updated due diligence records and revised risk classifications. Common triggers include:

- New information that contradicts existing customer data
- Transactions or behavior inconsistent with the known customer profile
- Emergence of new risk indicators or typologies

Following a triggered review, all internal records are updated to reflect any changes in the customer's risk status.

Periodic Risk-Based Reviews

Customer risk classifications also determine the schedule and scope of regular reviews:

- High-risk customers are reviewed annually. These reviews verify address, source of funds and wealth, media exposure, and account activity.
- Medium-risk customers are reviewed every two years. This includes refreshing due diligence documents and re-evaluating customer behavior and financial

activity.

- Low-risk customers are reviewed every three years. The process focuses on identity verification and screening for any newly emerged adverse data.

In addition, an ad hoc review may be initiated at any time if:

- New risk factors are detected
- Irregular or suspicious behavior is observed
- Regulatory or sector-specific developments require it

Adjustments Based on the National Risk Assessment (NRA)

The Company regularly aligns its monitoring activities with the latest National Risk Assessment published by the Curaçao authorities. Where new threats, typologies, or regulatory priorities are identified, the Compliance Officer updates the monitoring framework accordingly. Adjustments may include:

- Revising transaction monitoring thresholds
- Modifying alert settings and control processes
- Updating customer evaluation procedures based on revised risks

Commitment to a Dynamic Compliance Framework

By incorporating national and international risk intelligence into its monitoring processes, the Company ensures a dynamic compliance framework that adapts to emerging ML, TF, and PF threats. This approach promotes regulatory compliance and strengthens the platform's defenses against financial crime.

6. Risk-Based Approach

The Company implements a comprehensive and methodical risk-based strategy to identify, assess, and mitigate the misuse of its online gaming services for money laundering, terrorist financing, or the financing of weapons proliferation. This strategy aligns with the Financial Action Task Force (FATF) recommendations and involves both qualitative and quantitative evaluations of threats, system vulnerabilities, mitigation measures, and potential operational consequences.

A Business Risk Assessment (BRA) is conducted at least once per year, or whenever significant changes occur in the Company's operations, products, services, or regulatory environment. This assessment is formally documented, reviewed, approved by the Board of Directors, and updated as needed to address new risks and regulatory expectations.

Customer Risk

Customer activity is one of the Company's primary areas of financial crime exposure. Each customer is evaluated based on behavioral patterns, financial complexity, and geographical risk factors. Particular scrutiny is applied to customers identified as Politically Exposed Persons (PEPs), those with unclear or unverifiable sources of income, and customers whose transaction behavior deviates significantly from declared financial profiles.

- **Low-risk customers** typically exhibit consistent income, verifiable documentation, and transparent financial behavior.
- **High-risk customers** may show erratic or high-volume transactions, operate through opaque financial structures, or have connections to jurisdictions with weak financial oversight. These customers are subject to Enhanced Due Diligence (EDD) and intensified monitoring.

Product, Service, and Transaction Risk

Certain services and transaction types carry elevated risk levels, particularly those involving:

- Cryptocurrencies
- Prepaid cards or vouchers
- Digital wallets
- Peer-to-peer transfers

To control these risks, the Company employs:

- Automated transaction surveillance and anomaly detection
- Limits based on transaction size and frequency
- Real-time alerts for deviations in player or financial behavior

Controls are tailored to match each customer's risk profile and reviewed periodically.

Geographical Risk

Risk levels increase significantly when customers or counterparties are linked to countries with limited financial oversight, high corruption rates, or active international sanctions. The Company assesses country-specific risk based on data from sources such as FATF, CFATF, OFAC, the European Commission, the US State Department, and Transparency International.

Where geographical risks are present, the Company imposes:

- Mandatory Enhanced Due Diligence
- Manual approval of transactions
- Restrictions on account features such as deposits and withdrawals

Distribution Channel Risk

The method of customer interaction with the platform also influences risk. Online onboarding processes without face-to-face interaction are inherently riskier.

To mitigate this, the Company uses:

- Biometric identity verification tools
- Two-factor authentication
- Digital document validation via secure platforms

These measures apply uniformly across all customer access points to maintain consistent standards.

Technology-Related Risk

Before deploying new technologies or major system upgrades, the Company conducts formal risk assessments that include:

- Technical and operational risk analysis
- Identification of security vulnerabilities
- Development of mitigation strategies

- Evaluation of any residual risk

This applies to any updates involving new gaming functions, AI-driven systems, payment infrastructure, or blockchain applications. All findings are documented and made available to regulators upon request.

Sector-Specific Risk in Online Gaming

The Company acknowledges that online gaming has industry-specific vulnerabilities, including:

- Automated or high-frequency betting
- Exploitation of bonus or promotional systems
- Structuring withdrawals to disguise illicit funds

To prevent abuse, the Company enforces:

- Prohibition of unregulated or anonymous payment instruments
- Requirement to use licensed and approved financial institutions
- Monitoring and investigation of unusual gaming patterns or coordinated activity

Risk Mitigation and Monitoring Controls

To manage identified risks, the Company implements several risk-based controls, such as:

- Requesting supplementary documentation from customers
- Limiting account functions for higher-risk profiles
- Conducting monitoring tailored to each customer's risk score

Risk ratings are assigned during onboarding to both customers and Payment Service Providers (PSPs) and are reviewed periodically. Ongoing monitoring activities include:

- Screening against sanctions and adverse media sources
- Identification and review of PEP relationships

- Transaction pattern analysis against known customer profiles

Documentation and Reporting

The Company keeps secure records of:

- Risk classification decisions
- Due diligence actions taken
- Monitoring outcomes and triggered alerts
- Business Risk Assessment results

Where there is a reasonable suspicion of financial crime, the Company reports the incident promptly to the Financial Intelligence Unit (FIU) of Curaçao. Disclosure of such reports is prohibited and constitutes a serious violation of internal compliance policy.

Governance and Accessibility

All risk assessments, including the BRA and Customer Risk Assessments (CRA), are properly documented and contain analysis of inherent and residual risks by client type, product, and region. These records are regularly reviewed and can be made available to the Curaçao Gaming Control Board or other authorized entities as required.

7. Customer Due Diligence and Enhanced Due Diligence

Before initiating any business relationship, the Company must determine whether the prospective customer poses any risk related to money laundering, terrorist financing, or proliferation financing. This evaluation is fundamental to maintaining the platform's integrity and ensuring compliance with applicable legal and regulatory frameworks.

Customer Due Diligence (CDD) serves as the first line of defense, incorporating identity verification, financial and personal background assessments, risk scoring, and ongoing red flag monitoring. Open-source tools such as employment databases, property registries, insolvency reports, and social media profiles may be used to supplement this evaluation.

Where no elevated risks are identified, standard due diligence measures are applied. However, if high-risk factors are detected, such as links to high-risk jurisdictions or politically exposed persons (PEPs), Enhanced Due Diligence (EDD) is initiated immediately and without exception.

The Company employs a risk scoring model that evaluates key elements including geography, transaction history, service usage, and financial behavior. The process is strengthened through automated solutions and reliable third-party providers such as LexisNexis and WorldCheck. Additionally, biometric tools and secure identification technologies are utilized to verify identity and detect anomalies.

Anonymous or fictitious accounts are not permitted under any circumstances. All customers are required to provide verifiable identity documentation. If monitoring systems flag inconsistencies or risk indicators, the case is escalated to the Compliance Officer, who may initiate an internal report to the Financial Intelligence Unit (FIU) or alert law enforcement authorities if appropriate.

Customers are assigned to one of three risk tiers—low, medium, or high—based on factors such as transactional patterns, funding sources, and country risk exposure. Customers assessed as posing an unacceptable level of risk, as outlined in the Client Acceptance Policy, are refused or exited from the platform. Appendix IV provides additional guidance on risk classification criteria.

When CDD Measures Are Triggered

CDD is applied in the following circumstances:

- When a single or aggregated transaction equals or exceeds NAF 4,000
- When suspicious or irregular behavior is detected
- When customer documents appear incomplete, false, or suspicious
- When multiple transactions are linked and exceed the threshold
- When a risk profile shift occurs requiring deeper investigation

Core components of CDD include:

- Verifying the identity of the customer using reliable and independent sources
- Identifying beneficial owners and clarifying the control structure for legal entities
- Reviewing corporate relationships where applicable
- Ongoing monitoring of transactions in proportion to the customer's risk
- Verifying the source of funds where appropriate
- Prioritizing internal reporting duties when suspicious behavior is identified

Identity Verification and Information Collection

The Company requires the following information from all individual customers:

- Full name
- Date and place of birth
- Residential address
- Nationality
- Unique identification number

For low-risk customers, basic identity documentation may suffice. For high-risk customers, additional supporting materials are required to establish the individual's financial standing.

Accepted verification methods include:

- Government-issued IDs (passport or national identity card)
- Proof of address (e.g., bank statement or utility bill)
- Confirmation through email, phone, or postal validation
- Biometric authentication, IP analysis, or payment verification

If initial verification efforts fail, further steps such as live video verification or validation through regulated financial institutions may be applied.

For high-risk individuals, documentation relating to source of funds, source of wealth, and projected account usage may be requested. Medium and low-risk customers may provide occupational or business-related details, unless further review is warranted by the Compliance Officer.

Timing of CDD Implementation

CDD procedures are initiated at the earliest point of contact, ideally at the registration stage. Information submitted during onboarding is verified against trusted databases. If transactional activity equals or surpasses the NAF 4,000 threshold—whether through a single instance or cumulative actions—CDD must be completed in full.

Delays in completing CDD result in the following:

- Deposits and withdrawals are suspended
- Gameplay may proceed only with previously deposited funds
- Withdrawal attempts lead to account freezes

If CDD remains incomplete for more than 30 days:

- Where suspicion is present, a Suspicious Transaction Report (STR) is filed with the FIU
- If no red flags exist, funds are returned to the original funding source
- If risk concerns remain, the account may be terminated

All CDD activities are conducted with discretion. Employees are strictly forbidden from alerting the customer (“tipping off”) and are trained to protect the confidentiality of investigations.

Ongoing monitoring continues throughout the business relationship. Risk classifications are adjusted in response to new behavior, regulatory changes, or updates to client information. CDD must be re-applied when:

- Transaction volumes increase unusually
- A customer changes residence or country of operation
- The customer is identified as a PEP
- The NAF 4,000 threshold is met again
- Regulatory updates alter due diligence obligations

Legacy accounts are reviewed periodically, with priority given to those previously flagged as higher risk.

Where the verification process fails or a customer exceeds the Company’s acceptable risk threshold, the relationship is immediately discontinued. This decision is subject to Compliance Officer review and, where appropriate, an STR is filed with the FIU. All associated documentation is retained for at least five years following closure.

Use of Third Parties in CDD

The Company may rely on qualified external parties to assist in fulfilling certain CDD obligations, provided that such reliance is subject to strict contractual control. Ultimate responsibility for compliance with AML/CTF/CPF requirements remains with the Company.

Conditions for Third-Party Reliance

Before accepting CDD documentation from a third party:

- The provider must be governed by AML/CTF laws comparable to those of Curaçao
- A written agreement must ensure full and timely access to CDD files and results
- The Company must reserve the right to review or audit the provider's compliance processes

It is important to distinguish between *reliance* and *outsourcing*:

- In reliance, the third party performs CDD independently and shares the results
- In outsourcing, the third party operates under the Company's instruction and oversight

Evaluation and Oversight

Prior to onboarding a third-party provider, the Company assesses:

- The provider's legal and regulatory environment
- Past compliance record
- Technical systems and internal controls

Formal data-sharing agreements must clearly define responsibilities, access permissions, data protection requirements, and reporting protocols. Third parties are not permitted to make onboarding decisions on behalf of the Company.

Beneficial Ownership and Control Verification

When establishing relationships with corporate clients, the Company must identify and verify the ultimate beneficial owners (UBOs).

This includes:

- Identifying individuals who own or control 25% or more of the legal entity
- Where this is unclear, identifying those with operational or executive authority
- Investigating layered structures involving trusts, nominees, or complex entities
- Collecting and validating records such as corporate extracts, shareholder registries, and organizational charts

Where beneficial ownership cannot be confirmed, the most senior manager is recorded as the UBO in accordance with FATF recommendations.

All beneficial ownership data is verified using independent and credible sources. Related records are retained according to the Company's recordkeeping policy.

If a customer fails to cooperate with CDD or beneficial ownership inquiries, or deliberately obstructs verification efforts, the Company terminates the onboarding or business relationship. Such actions are considered serious red flags and may trigger additional reporting obligations.

8. Customer Acceptance Policy

The Company has implemented a structured Customer Acceptance Policy (CAP) that governs how individuals and entities are evaluated before they are permitted to access its regulated online gaming and betting platform. This policy is designed to prevent the misuse of the platform for illegal activities such as money laundering, terrorist financing, proliferation financing, fraud, circumvention of sanctions, and violations of regulatory provisions. The CAP ensures full compliance with the laws and rules applicable to Curaçao-licensed gaming operators.

This policy is a fundamental component of the company's overall AML, CTF, and CPF framework. It reflects the supervisory standards set by the Curaçao Gaming Control Board and is aligned with global benchmarks including the FATF recommendations, EU AML Directives, and relevant guidance from the Wolfsberg Group.

It is built upon the key legislative instruments of Curaçao, 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 employees, directors, contractors, and relevant third-party providers engaged in customer onboarding or ongoing customer management are required to comply with

this policy. No player is allowed to deposit, place bets, or initiate withdrawals before all customer due diligence obligations have been completed and the individual has been formally accepted as a client.

Scope of the Policy

The CAP is applicable to all individuals and legal entities that register to use the company's services, regardless of the channel used. This includes web-based access, mobile platforms, affiliate referrals, and third-party system integrations.

The policy remains active throughout the entire customer lifecycle, beginning with registration and continuing through to account closure or termination. It governs all gaming and betting products and services provided under the license OGL/2024/303/0300.

Eligibility and Access Requirements

Only individuals and entities that satisfy legal eligibility criteria are permitted to use the company's platform. Every applicant must confirm that they are of legal age, which must be at least 18 years or higher depending on the applicable jurisdiction. Registration requires the submission of accurate, verifiable personal information such as full name, date and place of birth, nationality, and a valid address.

Customers who are connected to jurisdictions listed on international sanctions registers or assessed as high-risk are not accepted. Screening is performed using globally recognized sanctions databases, including those issued by the UN, EU, OFAC, and OFSI.

Funds used by clients must be derived from legitimate, traceable sources. In cases that carry elevated risk, customers are required to provide documentation supporting their source of wealth or funds. The company reserves the right to reject applicants involved in behaviors such as chargeback abuse, bonus fraud, prior self-exclusion, or those with a history of regulatory infractions.

Risk-Based Onboarding Framework

The company follows a tiered, risk-based onboarding process. A risk classification is assigned upon registration based on factors such as employment, gaming and transaction behavior, geographic exposure, and historical activity.

- Customers assessed as low risk demonstrate transparent financial behavior and have stable profiles.
- High-risk customers may present with irregular activity, use complex financial arrangements, or be connected to high-risk countries or sectors.

- Politically Exposed Persons (PEPs), as well as their family members and close associates, are classified as high-risk by default.

Enhanced Due Diligence (EDD)

Where a customer is identified as high risk, the company applies enhanced due diligence measures. These include advanced verification procedures, tighter transaction controls, and ongoing scrutiny. EDD is automatically triggered in the following circumstances:

- The customer's income or financial profile cannot be validated.
- The individual is confirmed to be a PEP or is linked to one.
- Gaming behavior appears disproportionate to stated income levels.
- Payments are made using third-party methods or intermediaries.
- There are signs of multiple or linked accounts.
- Transaction patterns change significantly without clear justification.
- Large withdrawal requests are not supported by corresponding gameplay.

EDD requires senior-level approval and may include setting transaction limits or imposing further restrictions.

Geographic Risk Evaluation

The customer's location, source of funds, and place of transaction activity are analyzed for geographic risk. Reference sources include FATF, CFATF, OFAC, the European Commission, the US State Department, and Transparency International.

- Applicants from countries subject to sanctions are automatically declined.
- Clients from high-risk regions are subject to EDD and require specific compliance clearance.
- These accounts are closely monitored once onboarded.

Risk Evaluation Procedures

The risk classification process includes:

- Real-time screening at the point of registration using global watchlists.
- Assignment of a risk rating (low, medium, or high).
- Review and approval by the Compliance Officer for high-risk cases.
- Ongoing adjustments to risk scores based on emerging regulatory developments.

Product and Transaction-Based Risk

Some platform features and transaction types are inherently riskier, such as:

- Peer-to-peer transfers or in-game digital asset exchanges.
- Use of anonymous or loosely regulated payment tools like prepaid cards or cryptocurrency wallets.
- Repetitive deposit and withdrawal behavior with little gameplay.
- Use of unrelated or mismatched payment credentials.

These transactions are permitted only when the origin of funds can be verified. Any transaction deemed suspicious is escalated to the Financial Intelligence Unit (FIU). Inter-account transfers require prior compliance approval and are subject to close scrutiny.

Channel and Technology Risk

Remote digital onboarding presents certain risks, including identity fraud or impersonation. To address this, the company uses the following safeguards:

- Biometric-based identification verification.
- IP and device location checks.
- Multi-factor authentication processes.

Before any new technology or payment method is introduced, a formal risk review is conducted. Technologies that increase anonymity or obscure customer identity are subject to enhanced controls. All third-party providers involved in onboarding or payments are vetted for compliance history and operational integrity.

Defined Risk Dimensions and Controls

The company evaluates customer risk across four dimensions:

1. **Customer Profile Risk:** Includes red flags such as high turnover, intermediary use, multiple accounts, or income inconsistencies.
2. **Product and Transaction Risk:** Considers signs like third-party deposits, mismatched documents, and high-frequency switching of methods.
3. **Geographic Risk:** Considers connections to high-risk or sanctioned countries.
4. **Channel and Technology Risk:** Involves onboarding from unverified sources or use of unregulated partners.

A risk calculator is used to assign a numerical score to each customer. Depending on the score, the following controls are applied:

- **Low Risk:** Standard due diligence.
- **Medium Risk:** Additional document checks and enhanced monitoring.
- **High Risk:** Enhanced due diligence, compliance officer review, and continuous risk reassessment.

Each customer's risk classification is kept under review and updated as needed in response to behavioral changes or regulatory developments.

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, inheritance or	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 the Risk Indicators

The risk indicators outlined in the preceding section are applied by onboarding and compliance teams during client registration, ongoing monitoring, and scheduled profile reviews. Each indicator is assessed independently, then analyzed in context with the broader customer profile to determine the appropriate risk classification.

- Customers displaying mainly low-risk characteristics are subject to standard due diligence measures.
- Where a combination of low- and medium-risk features is identified, the Company imposes additional verification steps and increases monitoring intensity to reflect the elevated risk level.
- The presence of one or more high-risk indicators automatically triggers Enhanced Due Diligence (EDD), which must be completed before granting access to any services. These cases require formal approval by senior compliance personnel and may be subject to more frequent reassessments.

Risk classifications are dynamic and subject to change. They are reviewed on a recurring basis and adjusted as needed based on behavioral trends, system alerts, intelligence updates, or regulatory changes. This ensures the Company remains aligned with evolving financial crime risks and supervisory expectations.

Onboarding Procedures

The Company maintains a structured and well-documented onboarding framework designed to ensure that only customers who meet the required regulatory, compliance, and risk criteria are permitted to access its gaming services. No customer account is activated until identification, verification, and sanctions screening are fully completed.

Customer Registration and Identification

All applicants must submit accurate and verifiable personal data, including:

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

- Official identification number (e.g., passport or national ID)

Each individual is screened using automated systems connected to international sanctions databases and Politically Exposed Person (PEP) registries. Any matches are escalated for manual compliance review.

For customers assessed as high risk, the Company requires additional documentation such as:

- Recent bank statements reflecting consistent income
- Payslips or tax returns
- Financial statements for business or personal assets
- Contracts for asset sales
- Investment account summaries

These measures are designed to enhance onboarding integrity and mitigate the risk of financial crime.

Identity and Verification Requirements

All customers, including beneficial owners and authorized representatives, must meet strict identity verification standards.

Objectives of Document Verification

The purpose of document verification is to detect and prevent:

- Use of falsified or manipulated identity documents
- Attempts at impersonation
- Submission of digitally altered or screenshot-based files

Accepted identity documents must include:

- Full name
- Date of birth
- Unique identification number

- Issue and expiry dates
- A clear photograph
- Signature (where applicable)

Documents must be valid for at least one month beyond the submission date and must be undamaged, legible, and complete.

Upload and Validation Standards

Document submissions must adhere to the following criteria:

- Accepted formats: JPG, JPEG, PNG, or PDF
- Color images only
- Front and back visible where applicable
- Minimum resolution of 300 DPI or file size of 100 KB
- No obscured corners or cropped images
- No screenshots or altered digital copies
- Digital-only documents must be pre-approved

Image Authenticity Checks

The Company employs automated tools to validate the authenticity of uploaded documents. These tools perform:

- Metadata analysis
- File structure inspection
- Tampering risk scoring
- Comparison against official templates
- Font and layout consistency checks

Extracted data is cross-checked with internal databases and third-party verification systems.

Proof of Address (PoA) Verification

In-Person Clients

For face-to-face onboarding, the Money Laundering Compliance Officer (MLCO) inspects the original address document and retains a certified copy.

Remote Clients

For remote onboarding, the following steps are taken:

- Upload of a valid PoA document dated within the past 90 days
- Automated checks for structural integrity and template validation
- Verification using digital trust scores and mapping services such as Google Maps
- Manual review by compliance personnel

Accepted PoA documents include:

- Utility bills (electricity, internet, water)
- Bank or credit card statements
- Tax filings, lease agreements, or mortgage letters
- Official correspondence from employers or government bodies
- Voter registration documents or property deeds

Documents also accepted if containing a full address:

- Passport
- National identity card
- Driving license
- EU residence permit

Documents not accepted include:

- Mobile phone bills

- Prepaid card statements
- Medical or insurance correspondence
- Documents showing only a P.O. Box
- Records older than 90 days

One document cannot be used to verify both identity and address.

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

- **Source of Funds (SOF)** refers to the specific origin of deposits into a customer account.
- **Source of Wealth (SOW)** refers to the broader financial profile and overall asset base of the individual.

SOF and SOW checks are essential to understanding the customer's financial background and to preventing illicit financial activity. In high-risk cases, the Company requires extensive documentation to verify both sources.

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 Profits	or	Dividend statements, audited financial reports
Loans Investments	or	Loan agreements, transfer receipts, investment confirmations
Property or Asset Sales		Sales contracts, dealer confirmations, shipping documents, or customs declarations

Ongoing Monitoring

The Company recognises that initiating a business relationship is only the starting point of a broader compliance lifecycle. Maintaining up-to-date oversight of customer behaviour is essential to confirm ongoing alignment with assigned risk levels and to identify any changes that may heighten the risk of financial crime exposure.

Real-Time Monitoring

To ensure effective supervision, the Company operates real-time monitoring systems that evaluate customer activity continuously. These systems are designed to detect anomalies or suspicious patterns that may suggest platform misuse. Alerts are triggered in response to behaviours such as:

- Transactions that significantly differ from the customer's historical activity
- Fast movement of funds with little to no gaming participation
- Use of irregular or unrecognised payment tools, or frequent changes in payment methods
- Activity suggesting coordinated manipulation, bonus abuse, or economically unjustified value transfers

All flagged activity is escalated for manual review by trained compliance professionals. Where necessary, these cases may lead to internal investigations or formal reporting in accordance with regulatory obligations.

Periodic Risk-Based Reviews

In addition to automated oversight, the Company conducts scheduled customer reviews based on each individual's risk classification. These periodic evaluations aim to:

- Confirm that Know Your Customer (KYC) data remains accurate and current
- Detect changes in customer behaviour that might necessitate reclassification
- Apply enhanced verification procedures if new concerns arise

Triggering events that may prompt these reviews include:

- A customer relocating to or conducting transactions from a high-risk jurisdiction
- Significant increases in wagering activity, deposit volume, or withdrawal frequency
- Changes in funding sources, particularly if involving third parties or unregulated entities

Where risk levels increase, the Company updates customer classifications and may require submission of fresh documentation. Until verification is successfully completed, account restrictions may be temporarily applied.

Prohibited Clients and Transactions

To preserve the integrity of its services and comply with regulatory standards, the Company enforces strict limitations on client eligibility and permissible transaction types.

Unacceptable Conditions for Onboarding or Continued Service

The Company does not permit account creation or transaction processing for customers who:

- Refuse to submit identification or verification documents, except where a delay is justified and recorded
- Appear on official sanctions lists or watchlists issued by the United Nations, European Union, OFAC, OFSI, or Curaçao authorities
- Attempt to transact through institutions located in jurisdictions with inadequate regulatory controls, including shell banks or those allowing anonymous accounts

Further, no services are provided to individuals or entities suspected of involvement in:

- Terrorism as defined by applicable European Union directives
- Drug trafficking, in accordance with the 1988 United Nations Convention
- Organised criminal enterprises, human trafficking, or cybercrime
- Financial fraud, corruption, tax evasion, or currency counterfeiting

Immediate Rejection and Exclusion Criteria

The Company rejects customer applications or suspends accounts without delay in the following cases:

- Use of false or unverifiable identities, failure to complete verification within 30 days, or submission of forged documentation
- Engagement in prohibited industries, including arms trading, unlicensed digital asset businesses, or adult content services
- Residence in or transactions from countries or territories listed as prohibited or sanctioned
- Breaches of legal age requirements or falsified eligibility information
- Behaviour suggestive of collusion, bonus abuse, manipulation of platform functionality, or identity fraud
- Inability to verify source of funds or source of wealth, or evidence that such funds may derive from criminal origins

Prohibited Jurisdictions

In line with its internal compliance framework and applicable legal requirements, the Company imposes a strict restriction on customer sign-ups and transactions originating from specific jurisdictions. This includes both disputed regions and countries classified as high-risk, sanctioned, or otherwise incompatible with the Company's compliance standards.

Disputed or Unrecognised Territories

The Company does not establish business relationships with individuals based 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

Restricted Countries

Customer registrations and financial activity are blocked from the following countries:

- 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 from these countries are rejected automatically at the onboarding stage. Related transactions are blocked immediately. Rejections are recorded and preserved to meet the regulatory reporting standards in Curaçao.

Enhanced Due Diligence and Escalation Procedures

Customers who present a higher degree of financial crime risk are subject to Enhanced Due Diligence (EDD). This process is mandatory for politically exposed persons (PEPs), individuals tied to high-risk jurisdictions, or clients whose financial activity significantly exceeds expectations based on their declared background.

EDD Measures Include:

- Full assessment of financial background

- Verification of both the source of funds and source of wealth, supported by reliable documentation
- Collection of relevant records such as:
 - Financial statements
 - Tax returns and income slips
 - Contracts confirming asset sales
 - Investment account summaries
 - Proof of ownership for legal entities

All EDD files must be reviewed and signed off by senior compliance personnel. Where risk is elevated, decisions are escalated to the Board of Directors.

Once approved, high-risk clients are monitored more closely. This includes:

- Lower thresholds for triggering transaction reviews
- More frequent reassessment of risk classification
- Real-time behaviour monitoring through automated alerts

This multi-level approach supports strong risk control and ensures compliance with Curaçao's financial crime laws.

Prohibited Categories of Customers

The Company strictly forbids the onboarding or continued relationship with any individuals or entities that pose unacceptable legal, financial, regulatory, or reputational risks. The following types of customers are categorically excluded:

- Individuals using fake, anonymous, or misleading identities
- Clients who do not complete identity verification within 30 days
- Corporate entities with shell structures or unverifiable ownership information
- Persons or organizations listed on international or domestic sanctions databases

- Residents of, or those conducting transactions from, high-risk or prohibited regions
- Underage individuals who do not meet the minimum legal gambling age
- Customers with a known history of fraud, identity theft, bonus misuse, or suspicious activity
- Users funding accounts through anonymous or unverified third-party channels
- Individuals whose source of funds or wealth cannot be verified reliably

Triggers for Immediate Rejection or Suspension

The Company reserves the right to instantly decline any application or suspend existing customer accounts if any of the following conditions apply:

Identity and Documentation Triggers

- Inability or refusal to provide valid Know Your Customer (KYC) documents or proof of address
- Submission of altered, forged, or otherwise suspicious identification materials
- Persistent lack of response during the verification process

AML, CTF, and CPF Risk Triggers

- Positive matches with politically exposed person (PEP) or sanctions screening tools without suitable justification
- Strong indicators of involvement in financial crime
- Failure to establish a legitimate and credible source of funds

Behavioural and Transactional Red Flags

- Activity that does not align with the customer's stated financial profile
- Use of multiple or linked accounts, or unregistered payment instruments
- Efforts to circumvent compliance controls, exploit platform mechanisms, or coordinate fraudulent gameplay

- Repeated misuse of bonuses or signs of organized gameplay

Termination of Customer Relationships

The Company holds the authority to suspend or terminate any customer account when necessary to meet regulatory requirements or protect the integrity of its operations. Reasons for termination may include:

- Non-submission of required documentation within set timeframes
- Confirmed or suspected involvement in money laundering, terrorist financing, or proliferation financing
- Breaches of Curaçao's gambling regulations or the Responsible Gambling Policy
- Association with prohibited territories
- Providing false or deceptive information during onboarding or verification
- Financial conduct that does not match the customer's reported background
- PEP status where associated risks cannot be adequately mitigated
- Use of payment instruments owned by unrelated third parties
- Gambling activity by underage individuals or through identity misrepresentation

If the termination is connected to a suspected financial crime, the Company will file a Suspicious Transaction Report (STR) with the Financial Intelligence Unit (FIU) Curaçao in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds will be returned to the original payment method unless they are subject to legal freezing or seizure. Records of the termination and supporting materials will be retained securely for a minimum of five years.

Legal and Regulatory Compliance

The Customer Acceptance Policy is an essential component of the Company's broader framework for combating money laundering, terrorism financing, and proliferation financing. It fully complies with Curaçao's legislative and regulatory framework, 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
- The National Ordinance on Games of Chance (LOK)

These regulations are integrated into the Company's operational procedures throughout the customer lifecycle, from initial registration to account closure.

Responsible Gambling Integration

The Company incorporates its Customer Acceptance Policy into the implementation of its Responsible Gambling Policy. If customer behavior indicates a risk of harm or financial distress, the Company takes immediate preventive measures, which may include:

- Applying limits to deposits or losses
- Restricting access to services that carry a higher risk
- Temporarily or permanently suspending the customer's account
- Enforcing self-exclusion and applying restrictions across connected platforms

Customer service and compliance staff are trained to identify indicators of gambling harm and follow internal escalation processes accordingly.

Policy Oversight and Recordkeeping

The Customer Acceptance Policy is reviewed each year to ensure continued alignment with relevant legislation, updated risk assessments, and evolving industry standards. The review process is managed by the Compliance Officer and must be approved by the Board of Directors.

All related documentation is retained for at least five years following the end of the customer relationship. This includes:

- Identification and verification records
- Proof of address and documents verifying the source of funds
- Completed risk assessments and due diligence records
- Alerts and internal investigation logs

- Enhanced Due Diligence (EDD) records and account closure documentation

Access to these materials is restricted to authorized personnel and managed under the Company's data protection protocols.

9. Transaction Monitoring

The Company recognises that effective transaction monitoring is fundamental to its AML, CTF, and CPF compliance efforts. Given the fast-moving and high-volume environment of online gaming and betting, the potential for misuse is significantly heightened. To address this, the Company has established an advanced, technology-supported system that monitors, assesses, and responds to suspicious activity in real time.

Compliance with Curaçao Regulations

The Company's monitoring framework is fully compliant with applicable legislation in Curaçao, including the National Ordinance on the Reporting of Unusual Transactions (NORUT) and the Sanctions National Ordinance (SNO). It supports timely reporting to the Financial Intelligence Unit (FIU Curaçao) and ensures all escalation procedures are carried out in line with regulatory obligations.

System Architecture and Design

A real-time monitoring platform is in place, combining automated detection mechanisms with manual compliance oversight. This two-tiered system incorporates machine learning, customer behaviour modelling, and dynamic alert thresholds to identify irregular activity. When alerts are triggered based on preset criteria or detected anomalies, the Compliance team reviews and investigates as needed.

Examples of suspicious activity include:

- Large or erratic deposits that contradict the customer's known profile
- Use of several payment instruments, especially anonymous or loosely regulated ones
- Quick deposits and withdrawals with minimal or no actual gameplay
- Fund transfers between linked or associated accounts

- Transactions involving countries with weak AML frameworks or banking secrecy laws

Risk-Based Configuration and Scoring

Each transaction is measured against a set of risk parameters tailored to the customer's profile. These include transaction size, frequency, source of funds, and geographic indicators. A risk score is calculated, and alerts are generated when the score exceeds predefined levels.

Typical trigger scenarios include:

- Single or combined transactions amounting to NAF 4,000 or more
- Excessive or unusual deposit/withdrawal frequency
- Financial activity not aligned with declared income or verified sources
- Inconsistencies between IP location and declared country of residence
- Access from high-risk or restricted regions

When the NAF 4,000 threshold is reached, full Customer Due Diligence (CDD) is carried out, which may include renewed verification steps.

Monitoring Tools and Methodologies

The Company applies a combination of tools and methods to reinforce its monitoring program, such as:

- Geolocation filters to block access from restricted jurisdictions
- IP matching to detect multiple or linked accounts
- Speed checks to flag rapid fund movements
- Source of Funds checks comparing financial declarations with actual activity
- Behavioural profiling to detect changes in gaming patterns

The monitoring system continuously examines elements such as session duration, wager levels, win/loss ratios, device identifiers, and payment activity to build behavioural baselines and highlight anomalies.

Escalation and Reporting

When suspicious activity is confirmed, an internal Suspicious Activity Report (SAR) is prepared and escalated to the AML/CTF Officer. If warranted, a Suspicious Transaction Report (STR) is filed with FIU Curaçao under the NORUT regime.

All alerts, decisions, and associated documentation are timestamped and stored in accordance with regulatory audit requirements.

If CDD or Enhanced Due Diligence (EDD) cannot be completed because of missing or refused documentation, the customer's account is frozen and the relationship terminated. Remaining balances are returned to the original payment method, unless otherwise restricted by law or regulatory order.

10. Politically Exposed Persons (PEPs)

The Company acknowledges that individuals identified as Politically Exposed Persons (PEPs) present an increased risk of involvement in financial crimes such as money laundering or corruption. As part of its Enhanced Due Diligence (EDD) framework, the Company applies strict procedures when dealing with PEPs and those associated with them.

Definition of a PEP

A PEP refers to any person who currently holds, or has recently held, a high-profile public position. This includes, but is not limited to:

- Heads of state or government
- Senior political officials or members of parliament
- High-ranking judicial or military personnel
- Executives at state-owned enterprises
- Senior figures within international organisations

The same level of scrutiny is applied to:

- Close family members of PEPs
- Individuals known to be associates or business partners of PEPs

Onboarding Controls and Required Approvals

When a customer is identified as a PEP, either during the onboarding stage or through continuous monitoring, the Company activates a formalised risk assessment process. This includes:

- A full analysis of the individual's risk profile
- Verification of both source of funds and source of wealth
- Collection of documents that confirm the individual's financial background
- Escalation for senior management review and written approval before proceeding with account activation

No account connected to a PEP may be opened, maintained, or accessed without written authorisation from a senior manager.

PEP Register and Monitoring Procedures

All confirmed PEPs are documented in a dedicated internal register maintained by the Compliance Officer. This register contains:

- Full identity details of the customer
- Results of the risk assessment
- Details of any risk mitigation steps taken
- Documentation justifying the onboarding decision

The register is regularly reviewed and updated in response to any change in the PEP's status or associated risks.

Ongoing Oversight and Compliance Requirements

All PEPs are subject to:

- Continuous monitoring of their transactions and account behaviour
- More frequent reviews of their customer profile
- Lower thresholds for triggering internal alerts for unusual activity

These procedures are designed in accordance with applicable laws in Curaçao and the international guidelines issued by the Financial Action Task Force (FATF).

By enforcing these enhanced measures, the Company ensures that any relationship involving a PEP is properly controlled and that potential regulatory or reputational risks are mitigated through ongoing supervision.

11. Sanctions Policy

The Company is fully dedicated to complying with all relevant international sanctions laws and regulations. This policy describes the internal processes and safeguards used to detect, prevent, and mitigate exposure to sanctioned persons, entities, and jurisdictions. Sanctions are issued by national and international authorities as a tool to support foreign policy, protect national security, and uphold global standards in areas such as financial crime, terrorism, corruption, and human rights.

Types of Sanctions

Sanctions differ in nature depending on the issuing authority and may include various restrictions. The main categories are as follows:

Comprehensive Sanctions

These measures impose full restrictions on economic and financial dealings with specified countries or territories. The aim is to restrict access to global financial systems and economic resources.

Regime-Based Sanctions

These sanctions apply to government leaders, political parties, or public-sector organisations linked to corruption, abuses of power, or actions that threaten regional stability. Measures may involve trade controls, travel restrictions, or asset freezes.

Sectoral Sanctions

These target specific sectors within an economy, such as banking, defense, or energy. Unlike comprehensive sanctions, they apply to defined types of transactions or activities.

Debt and Equity Sanctions

These prohibit sanctioned parties from accessing financial markets by restricting the issuance or trade of securities, shares, bonds, or similar financial instruments.

Conduct-Based Sanctions

These are applied based on specific behaviour or activities, regardless of location or nationality. They typically target those involved in crimes like terrorism, arms trafficking, cybercrime, or large-scale corruption.

Some sanctions programs may contain multiple types of restrictions from the categories listed above.

Applicable Sanctions Frameworks

Due to the international reach of its services, the Company observes and adheres to several global sanctions frameworks.

United Nations (UN)

Sanctions imposed by the UN Security Council are mandatory for all member states. These are integrated into the Company's compliance controls and screening processes.

European Union (EU)

EU sanctions apply to:

- Individuals and companies located in EU member countries
- EU citizens operating abroad
- Companies established within the EU, including branches outside of Europe
- Transactions that have any EU link
- Aircraft and vessels under EU jurisdiction

The Company ensures that EU-related sanctions are consistently applied across all areas of operation.

United Kingdom (UK)

UK sanctions extend to:

- Activities within UK territory
- UK citizens and companies, including foreign branches
- Transactions conducted in part or in full through the UK

These restrictions are followed unless they directly contradict legally binding obligations within the European Union.

United States (US)

US sanctions include:

- **Primary sanctions**, which apply to US individuals, entities, and their foreign subsidiaries

- **Secondary sanctions**, which may be enforced against non-US parties engaging in prohibited activities that contradict US foreign policy interests

The Company applies US sanctions as far as they align with EU and Curaçao legal requirements. In cases of conflict, such as with the EU Blocking Statute, the Compliance Officer refers the issue to senior management and the Board for resolution.

Policy Commitments

In line with this policy, the Company shall:

- Freeze or block accounts where legally mandated
- Prohibit dealings involving sanctioned parties or jurisdictions
- End business relationships with sanctioned individuals or entities, unless restricted by governing law
- Detect and stop efforts to avoid or bypass sanctions controls
- Integrate sanctions compliance into customer onboarding, monitoring, and risk assessment practices

Consequences of Non-Compliance

Violating sanctions laws may result in serious regulatory penalties, criminal prosecution, and reputational damage. Any employee found responsible for non-compliance may face disciplinary measures, including possible termination. Every employee is expected to understand this policy, comply with it fully, and report any suspected breaches to the Compliance Officer without delay.

Roles and Responsibilities

Board of Directors

The Board holds overall responsibility for overseeing the Company's sanctions compliance efforts. This includes:

- Reviewing and approving the sanctions policy
- Promoting a strong culture of compliance
- Ensuring sufficient resources and staffing

- Reviewing reports related to sanctions from the Compliance Officer
- Appointing a qualified Compliance Officer and supporting their authority

Director(s)

Directors assist in handling complex sanctions issues, especially where legal or jurisdictional ambiguities are involved. They provide support and input in cases that carry significant risk.

Compliance Officer

The Compliance Officer is responsible for managing daily compliance with sanctions obligations. Their duties include:

- Conducting sanctions screenings on customers, transactions, and third parties
- Recommending updates to the policy when needed
- Keeping staff informed about relevant sanctions developments
- Ensuring accurate customer identity and screening data

All Employees

All employees are required to:

- Adhere fully to the Company's sanctions-related procedures
- Stay informed about the risks posed by individuals or entities subject to sanctions
- Immediately report any suspected breach to the Compliance Officer
- Refrain from providing advice that could aid customers in circumventing sanctions restrictions
- Complete required sanctions training within the designated timeframes

Sanctions Screening

Sanctions screening is embedded in both the onboarding process and ongoing customer monitoring. The Company uses an external screening solution that continuously syncs with real-time updates from official sanctions databases.

Match Classification

The screening platform categorises potential matches into the following types:

- **True Positive:** A direct and verified match with a sanctions listing
- **Potential Match:** A partial or ambiguous result that needs further manual review
- **False Positive:** A match initially flagged but ruled out after investigation
- **Non-Criminal Match:** A match involving someone listed for reasons unrelated to criminal activity
- **Unknown:** Cases where the available data is insufficient for conclusive evaluation

Confirmed matches and potential matches are escalated to the Compliance Officer for assessment. If the individual is rejected based on sanctions screening, the rationale and classification are logged.

Sanctions Lists Covered

The Company conducts screening against a wide range of international lists, including but not limited to:

- **European Union:** EEAS listings, CFSP consolidated registers, and sanctions related to Russia
- **United Kingdom:** HM Treasury consolidated list, Bank of England directives, and FCDO designations
- **United States:**
 - BIS lists, including Denied Persons, Entity List, and Military End User List
 - OFAC lists such as SDN, SSI, FSE, CAPTA, and various program-specific designations
 - Sanctions related to specific conduct or countries including Iran, North Korea, Cuba, Venezuela, and cybercrime
- **United Nations:** UN Security Council consolidated sanctions register

Screening is conducted both at account creation and throughout the customer relationship.

Response Protocol for Confirmed Matches

When a customer or transaction is verified as matching a sanctions entry, the Compliance Officer takes appropriate action. Depending on the circumstances, this may involve:

- Freezing or blocking customer assets
- Rejecting or discontinuing the relationship
- Imposing restrictions on transactions or services
- Escalating the case if there are legal conflicts or uncertainties

Sanctions Evasion

The Company acknowledges that efforts to evade sanctions are strictly prohibited and represent a serious compliance issue. Examples of evasion may include:

- Using unlisted intermediaries to process transactions on behalf of sanctioned persons
- Modifying payment details to hide the true parties involved
- Using VPNs or similar tools to mask geographic location
- Structuring transactions through shell entities to conceal involvement of blacklisted entities

Evasion attempts may be detected during onboarding, transaction monitoring, or general customer interactions. Any such suspicions must be promptly reported to the Compliance Officer. The officer will investigate the matter and determine whether escalation or formal notification is required. All findings must be properly documented and reported to senior management and the Board.

Asset Freezing

Freezing of assets, also referred to as blocking, is a standard legal obligation under most international sanctions regimes. If a customer is determined to have an ownership interest in funds and is under sanction, the Company is required to restrict access to those assets immediately.

Freezing does not involve transferring ownership. Rather, it prevents the customer from using, accessing, or benefiting from the assets unless special permission is granted by the appropriate authority.

This requirement applies to both fiat funds and virtual currencies. Freezing actions are implemented without delay once a match is confirmed and remain in force until legally lifted.

Sanctions Compliance Training

To ensure all personnel understand and uphold their obligations, the Company integrates sanctions compliance education into its broader training framework. The Compliance Officer is responsible for keeping the content up to date with regulatory changes and internal needs.

Two types of training are delivered:

- **General training** is required annually for all employees and covers fundamental sanctions knowledge and Company-specific responsibilities
- **Targeted training** is tailored to roles involving higher sanctions risk, including those working in onboarding, payments, monitoring, or compliance review

New employees must complete their initial training within 30 days of starting. Training content includes:

- Core features of sanctions regimes such as those of the UN, EU, UK, and US
- Types of sanctions and their practical implications
- Red flags that may indicate evasion attempts
- Responsibilities defined by internal policies
- Potential legal and disciplinary consequences of non-compliance

Training records are maintained and include course outlines, participant logs, test results, and attendance confirmation, all in line with regulatory retention requirements.

Outsourcing of Sanctions Compliance Activities

When sanctions screening or related services are outsourced, the Company remains fully accountable for ensuring that such activities meet all legal and internal standards.

Before entering into agreements with any third-party provider, the Company conducts due diligence to assess:

- The provider's technological capabilities and internal controls

- The provider's history of compliance with applicable regulations
- Reporting responsibilities and oversight mechanisms

The Compliance Officer maintains continuous oversight of all outsourced sanctions operations to ensure ongoing compliance with the Company's obligations.

Recordkeeping and Retention

All documentation related to sanctions compliance is retained in accordance with applicable legal requirements and the Company's internal retention policies. This includes:

- Results of all sanctions screening exercises
- Case files for investigated matches and their resolutions
- Records of training activities, including attendance and assessments
- Internal escalation records and external notifications
- Correspondence with regulatory authorities or sanctions bodies

These records are stored securely with access restricted to authorised personnel. All access is monitored and logged. Documents are retained for a minimum of five years following the end of the business relationship or the most recent related activity.

12. Suspicious and Unusual Activity and Transaction Reporting

The Company recognises that identifying and reporting suspicious or unusual activity is a vital part of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework. Timely detection and reporting are essential to prevent abuse of the platform and to ensure compliance with regulatory requirements in Curaçao.

Failure to report suspicious activity, whether due to oversight or deliberate inaction, can result in legal consequences, financial penalties, or reputational harm. The Company is committed to meeting its obligations under applicable laws and regulations, and to contributing to the broader fight against financial crime.

Detection of Suspicious or Unusual Activity

Unusual or suspicious conduct may be identified either through automated monitoring tools or observed directly by personnel. Common red flags include:

- Large, unstructured, or fragmented deposits and withdrawals
- Sudden shifts in transactional patterns without explanation
- Betting activity that deviates from normal gaming behaviour
- Use of the account in a way that contradicts the customer's risk profile
- Efforts to disguise the origin or movement of funds, particularly via intermediaries or third parties

While such activity does not always indicate criminal intent, all cases must be carefully assessed in line with the Company's internal review procedures.

Internal Escalation and Review Procedures

The Company follows a structured two-tier process for reviewing potentially suspicious transactions:

Preliminary Review

When a transaction is flagged by the monitoring system or reported by staff, an initial review is conducted to determine whether the activity can be reasonably explained or whether further examination is required.

Formal Assessment by AML/CTF Officer

If the suspicion persists, an internal Suspicious Activity Report (SAR) is submitted to the AML/CTF Officer. The Officer then evaluates whether the case should be escalated to the Financial Intelligence Unit (FIU) Curaçao for formal reporting.

All findings, decisions, and supporting documentation are logged and stored securely to comply with AML recordkeeping rules.

Filing of Unusual Transaction Reports (UTRs)

In accordance with Article 1 of the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Company is required to submit Unusual Transaction Reports (UTRs) to the FIU Curaçao through the goAML portal. This obligation applies to all licensed online gambling operators in Curaçao and has been in force since 1 January 2021.

The AML/CTF Officer is responsible for:

- Determining whether the activity qualifies as reportable under NORUT
- Submitting UTRs in a timely manner via the goAML platform
- Documenting the rationale and maintaining a full record of each submission
- Ensuring compliance with internal reporting protocols

Where the transaction involves serious concerns, the customer account may be temporarily suspended or permanently closed pending further investigation.

Employee Responsibility to Report

All employees are required to report any suspicion or concern that a customer may be involved in money laundering, terrorism financing, or other illegal conduct. This obligation applies even if the concern is based on partial information or limited context.

Reports must be submitted promptly to the AML/CTF Officer using the designated internal reporting system. Upon receiving a report, the Officer determines:

- Whether additional facts are needed to assess the situation
- Whether the matter should be reported to the FIU Curaçao
- What immediate measures should be taken to minimise risk and prevent further exposure

12.1 Monitoring for Suspicious and Unusual Activity

The Company evaluates both customer transaction behavior and inconsistencies in profile data to detect potentially suspicious conduct. A variety of warning signs may trigger internal scrutiny, including:

- Repeated reliance on anonymous payment instruments such as vouchers or prepaid cards
- Discrepancies between the customer's physical location and the source of their financial transactions
- Significant deposits followed by immediate withdrawal requests with little or no gaming activity
- Withdrawal attempts using payment methods not registered in the customer's name

- Efforts to evade verification checks or the use of false, proxy, or stolen identities
- Spending activity that conflicts with the customer's stated financial condition
- Frequent or unexplained changes to ownership or account details
- Delayed or incomplete submission of required due diligence documentation

Each case that raises concern is documented in full, capturing the relevant timestamps, transaction types, monetary values, and associated customer details. The Compliance and Fraud Prevention teams conduct a comprehensive analysis of the customer's profile and related data to determine if further escalation or official reporting is warranted.

12.2 Identification of Suspicious or Unusual Transactions

A transaction is considered unusual when it significantly diverges from the customer's established financial patterns or verified background, especially in the absence of a valid explanation. Examples include:

- Sudden increases in deposit or withdrawal amounts without a credible reason
- Use of accounts belonging to third parties or interactions with previously unrelated individuals
- Transactions that contradict the income or wealth level reported by the customer

The Company operates a real-time monitoring system to detect such anomalies. Alerts generated by the system are routed directly to the Compliance Officer for review. At the same time, staff members are trained to identify and report similar behavioral and transactional indicators using designated internal channels.

High-risk transaction types requiring closer review include:

- Transactions previously investigated or reported due to financial crime concerns
- Activity involving parties listed under the Sanctions National Ordinance or similar lists
- Single or grouped transactions totaling 5,000 Netherlands Antillean Guilders (NAF) or more within 24 hours, including deposits, bets, or withdrawals

Where reasonable suspicion exists that a transaction may be linked to money laundering, terrorist financing, or proliferation financing, immediate escalation to the

Compliance Officer is required. Prompt action ensures that threats are addressed and that reporting duties are fulfilled in a timely manner.

12.3 Timeliness of Reporting

Once a transaction has been reviewed and deemed suspicious or unusual, the Company must file an Unusual Transaction Report (UTR) with the Financial Intelligence Unit (FIU) of Curaçao in line with AML Regulation IV.1. This obligation applies even if the transaction was only attempted but not completed.

The Compliance Officer is solely authorised to file such reports and may do so without needing prior approval from other departments. Failure to submit a report in time is a violation of regulatory expectations and may result in legal consequences for the Company.

12.4 Confidentiality and Reporting Culture

All data associated with Suspicious Activity Reports (SARs) and Unusual Transaction Reports (UTRs) is treated as confidential. Employees are strictly forbidden from sharing the existence, progress, or contents of such reports with the customer involved or with any unauthorised person.

Any disclosure of this information is considered "tipping off" under Curaçao law and may hinder law enforcement investigations. Access to SAR-related materials is restricted to the Compliance Officer and a select group of approved personnel.

To enforce this standard, the Company incorporates specialised SAR confidentiality training into its AML and CTF learning programs. Any breach of these confidentiality protocols is addressed as a serious compliance matter and may result in disciplinary sanctions, including possible dismissal.

Commitment to Reporting Integrity

The Company actively promotes a culture of confidentiality, responsibility, and proactive risk management. This foundation enhances the effectiveness of the AML, CTF, and CPF program, maintains compliance with Curaçao's laws, and reinforces the Company's role in combating financial crime in the gaming industry.

13. Compliance Officer

The Company designates a dedicated Compliance Officer, who also serves as the appointed Money Laundering Reporting Officer (MLRO). This individual is primarily responsible for overseeing and implementing the Company's framework for Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF).

To ensure full independence and objectivity, this role operates separately from all commercial and operational departments. The Compliance Officer is granted direct access to internal systems, customer data, transaction records, and employees, and reports directly to the Board of Directors in line with Regulation V.3 of the Curaçao Gaming Authority's AML Guidelines.

Core Duties and Areas of Responsibility

Interaction with Regulatory Authorities

The Compliance Officer functions as the main liaison with relevant supervisory bodies, including the Financial Intelligence Unit (FIU) Curaçao. Responsibilities include:

- Filing Suspicious Activity Reports (SARs) through the goAML platform
- Responding to audit requests and regulatory compliance reviews
- Delivering quarterly updates to the Board regarding compliance risks, internal controls, and proposed policy changes

Enforcement of Policies and Procedures

The officer ensures the practical implementation and ongoing oversight of the Company's AML, CTF, and CPF protocols. This involves:

- Keeping policies in alignment with applicable laws and international benchmarks
- Updating procedures to reflect changes in regulations, internal risk exposure, or operational models
- Guaranteeing consistent application across all departments and services

Monitoring Transactions and Investigating Alerts

The Compliance Officer supervises both automated and manual systems for detecting financial irregularities. Responsibilities include:

- Reviewing alerts issued by monitoring platforms
- Investigating internal reports related to potential suspicious activity
- Deciding when to report cases to the FIU

- Retaining complete records of all reviews, conclusions, and supporting documentation

Staff Training and Awareness

The officer leads the development and rollout of training initiatives to ensure all staff understand their compliance obligations. This includes:

- Providing targeted instruction for employees handling onboarding, risk classification, or customer support
- Conducting yearly refresher training sessions across the Company
- Updating content to reflect legal changes or observed compliance gaps

Internal Reviews and Risk Analysis

As part of the Company's broader risk management strategy, the Compliance Officer:

- Carries out regular assessments of the AML framework
- Identifies weaknesses or inefficiencies within the control environment
- Designs and tracks the implementation of corrective actions

Recordkeeping and Documentation

The officer maintains structured and comprehensive records to support internal and external inspections. This includes:

- Documentation related to SARs, UTRs, and other compliance alerts
- Files related to due diligence and enhanced due diligence for customers
- Records of risk analysis, policy updates, and employee communications
- Logs of training sessions and internal audits

By maintaining these responsibilities, the Compliance Officer plays a key role in reinforcing the Company's regulatory compliance culture, reducing the risk of financial crime, and ensuring full adherence to Curaçao's legislative framework governing online gaming activities.

14. Senior Management

Senior management holds a vital role in sustaining the effectiveness of the Company's Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) measures. The Board of Directors is responsible for ensuring that executive leadership remains fully engaged in overseeing financial crime risks and actively supports the development of internal systems designed to mitigate these risks.

The AML/CTF Officer is tasked with regularly updating the Board on key developments that influence the Company's risk exposure or control frameworks. This includes the presentation of a detailed annual compliance report that evaluates the performance of AML, CTF, and CPF measures and identifies areas where enhancements may be necessary.

Annual and Quarterly Policy Oversight

Senior management is ultimately responsible for confirming that AML, CTF, and CPF policies, along with related procedures, are reviewed at least once per year. These reviews are supported by monthly risk evaluations, which help identify weaknesses in internal controls, inefficiencies in operations, or changes in the external threat environment.

If risk assessments or changes in regulation necessitate updates to existing policies, the AML/CTF Officer proposes such amendments to the Board. The Board then evaluates and approves the updates as appropriate, ensuring that the Company's controls stay aligned with both regulatory requirements and its own risk appetite.

Oversight of Employee Training

Executive leadership also oversees the Company's training initiatives on AML compliance. All staff members, especially those working in high-risk areas such as compliance, finance, or customer support, must receive training at regular intervals to ensure they are prepared to identify, address, and report suspicious activity.

Senior management ensures that training content remains accurate and up to date. The materials are revised to reflect changes in applicable law, new financial crime typologies, and the Company's operational context. Training is structured to enhance staff awareness of suspicious behavior, strengthen due diligence capabilities, and reinforce reporting procedures.

Internal Controls and Governance Standards

Senior leaders are responsible for maintaining a strong internal control framework. This includes enforcing proper separation of duties, ensuring that user access is appropriately limited, setting clear approval procedures, and maintaining real-time monitoring mechanisms to detect and address non-compliant activity.

All decisions, operational controls, and internal evaluations are recorded and documented to support transparency and provide a comprehensive audit trail. These practices ensure regulatory readiness and full traceability of financial crime prevention efforts.

Independent Audit and Assurance

To uphold the reliability of the AML, CTF, and CPF programme, senior management commissions periodic independent audits in line with Section V.5 of the AML Guidelines issued by the Curaçao Gaming Authority. These reviews assess the structure, implementation, and operational effectiveness of compliance systems.

Audit reports are delivered to the Board for review. Where deficiencies are identified, corrective actions are introduced and monitored until resolution. This continuous review process enhances the Company's ability to adapt to new risks and strengthens the long-term sustainability of its compliance framework.

15. Employee Training and Screening

Employees are an essential line of defense in the Company's efforts to prevent financial crime and meet regulatory obligations. To support this responsibility, the Company enforces a robust screening process for staff and provides targeted training that promotes awareness, ethical conduct, and compliance with its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) responsibilities.

Employee Screening Programme

A structured screening protocol is implemented in line with Regulation V.4 of the AML Guidelines issued by the Curaçao Gaming Authority. This protocol applies both at the point of recruitment and throughout employment, especially for staff in roles related to compliance, finance, risk management, or customer onboarding.

Pre-Employment Screening

Before any hiring decision is finalised, the Company ensures that shortlisted applicants are subject to the following checks:

- Verification of identity and legal work status using valid government-issued documents
- Criminal record screening to identify any prior misconduct involving financial crimes
- Reference and employment history checks to confirm the candidate's reliability and competence
- Screening through recognised sanctions and Politically Exposed Persons (PEP) lists using an approved external service

Applicants who do not meet the Company's integrity standards or pose a compliance risk are excluded from the hiring process.

Continuous Screening of Employees

After hiring, the Company maintains oversight of employee integrity through:

- Annual re-screening for those in roles with heightened exposure to financial crime risks
- Additional checks triggered by internal concerns, investigations, or changes in job function
- Ongoing monitoring of employees for developments such as sanctions listings, PEP associations, or legal issues

All screening-related data is handled securely and retained for at least five years, in line with data protection standards.

AML Training and Staff Awareness

Employees whose responsibilities intersect with the Company's AML, CTF, or CPF controls must complete mandatory training at onboarding and participate in refresher sessions each year. The content is tailored to specific roles and designed to equip personnel with the skills to identify, assess, and report suspicious or unusual conduct.

Training Topics Include:

- Legal obligations under Curaçao's AML, CTF, and CPF legislation
- Detection of suspicious behaviour, such as:

- Unusual betting or transactional patterns
- Use of anonymous or third-party payment instruments
- Discrepancies between claimed and observed financial activity
- Correct procedures for filing internal Suspicious Activity Reports (SARs)
- The importance of confidentiality during investigations and safeguarding client data

Employees are clearly informed that failing to follow internal compliance procedures, including delayed or incomplete reporting of suspicious conduct, may result in disciplinary measures, including dismissal or legal consequences.

Reporting and Escalation Procedures

All staff members are required to report suspicious or irregular activity to the Compliance Officer without delay, using the established reporting system. Structured templates and procedures are provided to ensure accuracy, confidentiality, and completeness of internal reports.

Confidentiality and Data Protection

Preserving confidentiality is a core principle of the Company's compliance approach. Staff are strictly prohibited from sharing any information related to SARs, investigations, or unusual transaction reports with unauthorised individuals. Any form of disclosure, including tipping-off, is treated as a violation of Curaçao law and may result in disciplinary action.

Culture of Compliance

Through regular screening and role-specific training, the Company ensures its staff are equipped to support its risk management and compliance objectives. Employees are expected to act as responsible compliance partners and contribute to the Company's efforts to detect, prevent, and report financial crime within its operational scope.

16. AML Compliance Audit

The Company considers internal auditing an essential function in ensuring the strength, reliability, and regulatory compliance of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) framework. Audits are viewed not as procedural obligations but as key governance tools

that enhance transparency, accountability, and operational efficiency. All audit outcomes are formally reported to senior management and the Board of Directors for timely evaluation and resolution.

Frequency and Audit Triggers

The Company conducts AML compliance audits at regular intervals, with at least one formal review completed every year. Additional audits may be scheduled following major regulatory updates, internal restructuring, or any event that highlights potential weaknesses within the compliance framework. These audits are led by qualified internal or external professionals who are independent from daily compliance operations and have specific expertise in financial crime risk management.

Scope of the Audit

Each audit assesses the overall performance and adequacy of the Company's compliance framework. Areas under review typically include:

- **Policies and Procedures**
Evaluation of whether AML, CTF, and CPF policies are current, legally compliant, and consistently implemented across departments.
- **Risk-Based Approach**
Examination of the Business Risk Assessment (BRA) and Customer Risk Assessment (CRA), including risk scoring methodology and corresponding mitigation strategies.
- **Transaction Monitoring and Reporting**
Review of how effectively the monitoring system detects suspicious transactions and the quality and timeliness of Suspicious Activity Reports (SARs).
- **Customer Due Diligence (CDD) and KYC/KYB**
Assessment of identity verification processes, beneficial ownership checks, and adherence to internal recordkeeping standards.
- **Sanctions Screening Controls**
Verification of the accuracy and performance of screening tools used to identify matches against global sanctions databases.
- **Employee Training and Background Checks**
Review of staff training coverage and relevance, along with the effectiveness of employee screening protocols for sensitive roles.
- **Information Technology and Data Security**
Inspection of technical controls in place to secure compliance systems,

risk-scoring engines, and user access permissions.

Reporting and Remediation

After each audit, a formal report is prepared and submitted to senior management and the Board, in accordance with Section V.7 of the AML Guidelines issued by the Curaçao Gaming Authority. This report highlights any weaknesses or gaps, and outlines corrective actions with target completion deadlines.

If critical issues are identified, the Compliance Officer is responsible for ensuring that corrective actions are taken without delay. Follow-up audits may be initiated as necessary to confirm the effective resolution of identified deficiencies and to ensure risk has been reduced to acceptable levels.

Documentation and Regulatory Readiness

All documentation related to compliance audits is retained securely for a minimum of five years. These records are made available to the Gaming Control Board (GCB) or other relevant authorities upon request. This practice demonstrates the Company's ongoing commitment to regulatory transparency and continuous improvement in its financial crime prevention efforts.

17. Regulatory Access and Cooperation

The Company confirms its full commitment to maintaining transparent and cooperative relationships with the Curaçao Gaming Control Board (GCB) and other competent supervisory, regulatory, or law enforcement authorities. This cooperation is recognised as a core aspect of sound corporate governance and a fundamental component of the Company's compliance infrastructure.

Access to Systems and Documentation

To enable effective regulatory oversight, the Company provides regulators with complete and unrestricted access to its systems, records, personnel, and processes. This applies to both scheduled supervisory audits and unannounced inspections, whether conducted remotely or on-site.

Upon request, the Company makes the following information available:

- Records of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)
- Full transaction histories, including deposits, wagers, and withdrawals

- Internal and external AML, CTF, and CPF risk assessments
- Compliance manuals, internal policies, and standard operating procedures
- Training records and internal compliance-related communications
- All Suspicious Activity Reports (SARs), whether internal or submitted
- System-generated audit trails and platform access logs

The Company ensures all requested materials are delivered promptly, accurately, and in full. This includes facilitating live walkthroughs of relevant systems and providing additional explanations or documentation when required to support inspections or technical reviews.

Record Retention and Data Security

All compliance-related records are retained for a minimum of five years, or longer where legally required. The Company stores these records in secure, access-controlled environments to protect them from tampering, loss, or unauthorised access. Records remain accessible for inspection and traceable throughout their lifecycle.

Response to Inspection Findings

The Company commits to responding efficiently and effectively to any findings or recommendations made by the GCB or other regulatory bodies. This includes:

- Implementing corrective measures within the agreed deadlines
- Submitting follow-up documentation or status updates upon request
- Providing supporting evidence to confirm implementation of required changes

All correspondence with regulators is formally recorded, and follow-through on all actions is tracked internally to ensure accountability.

Recognition of Supervisory Authority

The Company formally acknowledges the authority of the GCB to conduct supervisory examinations in accordance with Section V.6 of the Curaçao Gaming Authority AML Guidelines. The Company recognises its duty to cooperate fully during any examination and to grant access to relevant systems, records, and personnel. It also accepts the GCB's right to evaluate the adequacy and performance of its AML, CTF, and CPF framework and to impose measures where material weaknesses or non-compliance are identified.

Governance and Compliance Culture

The Company embeds regulatory engagement into its wider governance model. Senior management actively supports transparent, timely, and cooperative interactions with oversight bodies. By fostering a culture rooted in compliance, integrity, and openness, the Company reinforces the effectiveness of its financial crime prevention framework and contributes to maintaining the integrity of Curaçao's licensed gaming environment.

18. Internal Audit and Reporting

The Company maintains a dedicated internal audit function that operates independently to assess the effectiveness, efficiency, and resilience of its Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) compliance framework. Internal audits are treated as essential governance tools rather than routine formalities. At a minimum, one audit is conducted annually, with additional audits initiated in response to changes in operational structure, emerging risks, or revised regulatory requirements.

Audits are performed either by internal audit staff or by qualified external professionals when a higher degree of independence or specialised expertise is required. These professionals have no operational involvement in daily compliance activities, ensuring objectivity in the audit process.

Scope of Audit Activities

Each internal audit involves a comprehensive evaluation of the following components:

- The adequacy, implementation, and regulatory compliance of AML, CTF, and CPF policies and procedures
- Effectiveness of transaction monitoring and sanctions screening mechanisms
- Quality, completeness, and timeliness of Suspicious Activity Reports (SARs)
- Customer onboarding and due diligence practices, including customer risk scoring and the application of enhanced due diligence where appropriate
- Relevance, frequency, and overall effectiveness of AML training programs
- Governance oversight, internal controls, and data retention procedures
- The consistency of internal controls with the Company's risk appetite and legal obligations

Reporting and Remediation Process

At the conclusion of each audit, a detailed report is submitted to senior management and the Board of Directors or, where applicable, to a designated oversight committee. The report includes:

- The audit methodology and scope
- Key findings and any identified weaknesses or gaps
- Recommendations for remediation
- Deadlines for implementing corrective actions

Senior management is accountable for ensuring that all audit recommendations are addressed within the specified timeframes. Implementation progress is documented and tracked until full resolution is achieved.

Compliance with CGA AML Guidelines – Section V.5

The Company ensures compliance with Section V.5 of the AML Guidelines issued by the Curaçao Gaming Authority by maintaining an audit function that is operationally distinct from the compliance department. The audit function is staffed with professionals who possess the necessary expertise in financial crime risk management. Audit reviews are designed to assess both the design and actual implementation of the Company's AML, CTF, and CPF controls.

Findings are formally presented to the Board, and deficiencies are subject to structured remediation plans with documented follow-up actions. Audit areas include:

- The effectiveness of Business Risk Assessments (BRA) and Customer Risk Assessments (CRA)
- Execution and documentation of Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)
- Oversight of transaction monitoring alerts and red flag handling
- Procedures for identifying and escalating suspicious activity
- Sanctions screening systems and match-handling protocols
- AML training delivery, content quality, and employee engagement

Recordkeeping and Auditor Access

All records related to internal audits, including working papers, final reports, supporting evidence, and remediation documentation, are retained for a minimum of five years or longer if legally required. These records are stored securely in environments with restricted access to prevent unauthorised use, tampering, or data loss.

Auditors are granted full access to all necessary systems, documentation, and personnel. This ensures that audit activities meet the standards expected by regulators and support the comprehensive oversight of the Company's financial crime prevention framework.

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: Client Risk Calculator

Customer Risk Calculator

Client no.:

Name:

NEW total score:

0.00

NEW risk level:

Low

Onboarding specialist:

Last update date:

Category

Score

low

0-2

medium

2 to 4

high

4 to 6

unacceptable

At least 1 unacceptable

Risk Category

Question

Risk score

Risk level

Additional comments

Customer's Age

Client

Citizenship

Geography

Second Citizenship (if any)

Geography

Country of Birth

Geography

Country of Residence

Geography

Does Customer have the status of PEP/RCA (Politically Exposed Person/Relative and Close Associate)?

Client

PROFILE

Purpose of account registration?

Client

Client

Client

SOF/ SOW

Source of funds

Client

Client

Client

Client

Client

Client

average

Source of wealth

Client

Client

Client

Client

Client

Client

average

INCOMING PAYMENTS

Average frequency of transactions

Transactions

Expected total value of transactions per period (NAP)

Transactions

Types of incoming payments

Transactions

Transactions

Transactions

Transactions

Transactions

Transactions

Transactions

average

OUTGOING PAYMENTS

Average frequency of transactions

Transactions

Expected total value of transactions per period (NAP)

Transactions

Types of outgoing payments

Transactions

Transactions

Transactions

Transactions

Transactions

Transactions

Transactions

average

Reasons for outgoing payments

Transactions

Transactions

Transactions

Transactions

average

BEHAVIOUR

Please indicate services of interest

Products and Services

Products and Services

Products and Services

Products and Services

Products and Services

Products and Services

average

CONFIRMATIONS

Channels

Payment Channels

Third-party involvement

Access

Onboarding

Adverse media level

Client

average

Manual risk level adjustment based on the specialist judgement (to 5)

Other

Comment regarding manual risk adjustment:
Summary of the applicant:

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	

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 V.4
- **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: