

Rapture B.V.

a Company with registered address at
Kaya Richard J. Beaujon Z/N Landhuis Joonchi II Curacao,
registration number 156074, domain name: zaza.com
(hereinafter referred to as “**Company**”)

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND PROLIFERATION FINANCING POLICY AND PROCEDURES

Stanislav Andrieiev, the
MLRO & Compliance
Officer

**Gouloud Mercedes
Hammoud** obo Guardian
Corporation Curacao B.V.,
Statutory Director

CONTENTS

1.	Policy Statement and General Provisions.....	4
2.	Purpose of the AML/CFT/CPF Policy and Procedures.....	4
3.	Audience.....	4
4.	Key Definitions.....	5
5.	Policy Implementation and Business Risk Assessment.....	6
6.	Customer Risk Assessment (CRA).....	8
7.	Customer Acceptance Policy.....	9
8.	Customer Due Diligence.....	14
9.	Ongoing Monitoring.....	20
10.	Reliance on Third Parties for Customer Due Diligence.....	23
11.	Risk Profiles.....	23
12.	Cryptocurrency.....	25
13.	Compliance and consequences of non-compliance: Termination of business relationship and asset freeze.....	25
14.	Beneficial Ownership and Third-Party Verification.....	27
15.	Reporting Procedures and Obligations.....	28
16.	Technological Development Risk Assessment.....	34
17.	Awareness and Training.....	34
18.	Audit.....	38
19.	Cooperation with Authorities.....	39
20.	Additional Measures.....	39
21.	Customer Notifications.....	40
22.	Applicable Rules and Legislation.....	40
23.	Policy Updates and Sanctions Monitoring.....	41
24.	Contact Information.....	42
25.	Policy Revision History.....	42
26.	Appendix.....	43

KEY INFORMATION

Approving Official(s):	Stanislav Andrieiev, the MLRO & Compliance Officer Gouloud Mercedes Hammoud obo Guardian Corporation Curacao B.V., the Statutory Director
Responsible Office:	Stanislav Andrieiev, the MLRO & Compliance Officer
Effective Date:	17.06.2025
Next Review Date:	17.06.2026

1. Policy Statement and General Provisions

Rapture B.V. is firmly committed to safeguarding its products, services, and operations from being exploited for money laundering, terrorist financing, or any form of criminal conduct. This **AML/CFT/CPF Policy and Procedures** document outlines the guiding principles and operational framework the Company follows to ensure adherence to all relevant laws, regulations, and international compliance standards.

This policy applies universally to all clients of Rapture B.V., regardless of their geographic location. It governs every aspect of the business, including but not limited to customer onboarding, transaction monitoring, unusual activity reporting, and ongoing due diligence.

Rapture B.V. employs a **risk-based approach** to identify, assess, and mitigate AML/CFT/CPF risks. To support this approach, the Company implements internal controls, mandatory employee training, and regular reviews to ensure compliance and continuous improvement of its AML/CFT/CPF measures.

2. Purpose of the AML/CFT/CPF Policy and Procedures

The primary objective of this policy is to establish a structured and effective system for detecting, preventing, and reporting activities that may be indicative of money laundering or the financing of terrorism on Rapture B.V. platform.

As a licensed operator in the online gambling industry, **Rapture B.V.** is bound by a wide array of national and international anti-money laundering and counter-terrorist financing regulations. Strict compliance with these regulations is essential not only for preserving the integrity of the financial ecosystem and maintaining public confidence but also for safeguarding the Company's licensing status and operational viability.

This policy aims to:

- Prevent the misuse of Rapture B.V. platform for the laundering of illicit funds or the facilitation of terrorism financing
- Define transparent procedures for **Know Your Customer (KYC)** processes, transaction monitoring, risk evaluation, and unusual activity reporting
- Ensure full compliance with regulatory requirements, including **Customer Due Diligence (CDD)**, **Enhanced Due Diligence (EDD)**, record retention, and timely reporting to the appropriate authorities
- Shield the organization from legal liabilities, reputational harm, and financial losses

By maintaining a robust AML/CFT/CPF compliance framework, **Rapture B.V.** reinforces its commitment to ethical business practices and supports the global fight against financial crime.

3. Audience

This **AML/CFT/CPF Policy and Procedures** applies to all individuals and entities directly or indirectly involved in the operations and service delivery of **Rapture B.V.** The following stakeholders are obligated to understand, adhere to, and implement the principles and processes outlined in this policy:

- **All Employees:** Including permanent, temporary, and contract staff engaged in customer onboarding, payment processing, risk management, compliance, or support functions.
- **Senior Management and Directors:** Accountable for ensuring compliance with AML/CFT/CPF obligations both at the strategic and operational levels.
- **Compliance Officers and Designated AML Personnel:** Responsible for the execution, supervision, and enforcement of AML/CFT/CPF controls and reporting mechanisms.
- **Customer Support and Operational Staff:** Tasked with conducting customer due diligence, transaction monitoring, and escalation of unusual activities.

- **Third-Party Service Providers:** Such as KYC/identity verification vendors, payment service providers, and customer onboarding partners who handle or process customer data or transactions on behalf of **Rapture B.V.**
- **Subcontractors and Consultants:** Engaged in any capacity related to customer engagement, platform management, or financial operations.

All parties listed above must be thoroughly familiar with and operate in full compliance with this policy to meet legal and regulatory obligations and to preserve the operational integrity and reputation of the Company.

4. Key Definitions

For the purpose of this policy, the following terms are defined as follows:

- **AML (Anti-Money Laundering):** Measures and procedures designed to detect and prevent the laundering of proceeds derived from criminal activity.
- **CFT (Combating the Financing of Terrorism):** Measures to detect, prevent, and report the financing of terrorist activities or organizations.
- **CPF – Combating the Proliferation Financing**
- **Company:** Refers to **Rapture B.V.**, a legally registered entity under the laws of Curaçao (registration no. 156074), located at Kaya Richard J. Beajon Z/N Landhuis Joonchi II, Curaçao.
- **Money Laundering (ML):** The process of disguising the origins of illicitly obtained funds to make them appear legitimate. This typically involves three stages:
 - **Placement:** Introducing illegal funds into the financial system, often through cash deposits, especially in jurisdictions with weak AML controls.
 - **Layering:** Concealing the origin of funds through complex transactions and transfers to obscure the audit trail.
 - **Integration:** Reintroducing the laundered funds into the economy as seemingly legitimate assets.
- **Terrorist Financing (TF):** The provision or collection of funds intended to support terrorist activities. Unlike money laundering, these funds may originate from both legal and illegal sources. The primary objective is not profit, but the operational support of terrorism.
- **Know Your Customer (KYC):** The process of verifying a customer's identity, assessing their risk level, and understanding their financial behavior to prevent money laundering and terrorist financing.
- **Customer Due Diligence (CDD):** Standard procedures used to gather and verify customer identity information and assess potential risks posed by a client relationship.
- **Enhanced Due Diligence (EDD):** Stricter verification measures applied to high-risk customers, including Politically Exposed Persons (PEPs) or clients from high-risk jurisdictions.
- **Politically Exposed Person (PEP):** An individual holding or having held a prominent public position, along with their close associates and immediate family members, due to the heightened risk of corruption.
- **Proliferation of Weapons:** The transfer or export of nuclear, chemical, or biological weapons, delivery systems, or related materials. Disrupting such proliferation is critical to counterterrorism efforts and often overlaps with anti-terror financing measures.
- **Unusual Transaction Report (UTR)** - is a formal notification submitted to the FIU Curaçao by a reporting entity, in accordance with the National Ordinance on the Reporting of Unusual Transactions (NORUT).
- **Financial Intelligence Unit (FIU):** A national body responsible for receiving, analyzing, and disseminating financial intelligence related to suspected criminal proceeds or terrorism financing.

- **Beneficial Owner:** The natural person(s) who ultimately owns or exercises control over a client and/or on whose behalf a transaction is executed.
 - **Risk-Based Approach (RBA):** A methodology for prioritizing AML/CFT/CPF measures based on the level of risk associated with a particular customer, product, transaction, or geographic location.
 - **Sanctions List:** An official list issued by government or international bodies (e.g., United Nations, OFAC, European Union) identifying individuals, entities, or countries subject to economic or financial restrictions.
 - **XCG** - Caribbean Guilder, Curacao currency.
-

5. Policy Implementation and Business Risk Assessment

Overview of Risk Exposure

Rapture B.V. recognizes three core areas of AML/CFT/CPF risk exposure:

1. **Reputational Risk** – Potential damage to the Company’s credibility and market perception
2. **Regulatory Risk** – Risk of non-compliance with applicable AML/CFT/CPF laws and regulations
3. **Litigation Risk** – Exposure to legal action arising from lapses in AML/CFT/CPF

controls To mitigate these risks, the Company’s AML framework focuses on six critical pillars:

- **Customer Identification Procedures**
- **Comprehensive Record-Keeping**
- **Internal Operational Procedures**
- **Employee Education, Training, and Development**
- **Robust Internal Controls and Communication Protocols**
- **Ongoing Evaluation of Procedures and Control Mechanisms**

Handling Proceeds of Crime

Regardless of the method used to transfer funds to any of the Company’s platforms, there is a continual risk that such funds may originate from illicit sources—including card fraud, theft, or drug trafficking. By applying heightened scrutiny and monitoring to high-spending customers, the Company seeks to effectively manage and minimize this risk.

High-Risk Products and Services

Certain products and services are deemed inherently riskier due to their attractiveness to money launderers and criminals. These include:

- Funds potentially originating from criminal activities
- Use of casino accounts solely for deposits/withdrawals without substantial gambling activity
- Specific games with high laundering potential (e.g., even-bet games like roulette or craps)
- Peer-to-peer gaming formats
- Transactions involving third-party bank accounts or cards
- Use of multiple player accounts or wallets
- Frequent changes to linked financial accounts
- Identity theft or impersonation for account setup
- Participation in shared gaming networks with multiple operators
- Use of unregulated or opaque e-wallets
- Complex or layered transaction structures

- Anonymous or unverified accounts
- Irregular or inconsistent betting patterns
- Use of cryptocurrencies or other digital payment systems
- High-risk distribution channels, particularly those lacking strong identification protocols

While non-face-to-face interactions are no longer automatically considered high risk, they still demand increased vigilance. Unless supported by robust identity verification technologies, these interactions should be treated with caution during risk evaluation.

Engagements involving third parties—especially those outside AML-regulated frameworks—also elevate the risk profile of customer relationships.

Due Diligence Risk Indicators

Indicators identified during the CDD process may include:

- Multiple gambling accounts or wallets used to mask transaction activity
- Frequent switching of bank accounts to disrupt monitoring patterns
- Use of stolen identities or financial data to create or access accounts
- Reliance on prepaid cards, which offer limited traceability
- Use of anonymous or minimally regulated e-wallets
- Participation in gaming platforms shared across multiple operators

Interpreting Risk Designations

Assigning a customer a high-risk status does **not** imply criminal intent or activity. Likewise, labeling a customer as low risk does not guarantee that no risk exists. Staff must apply sound judgment, maintain awareness, and follow the Company's risk-based procedures. When uncertainty arises, they must consult the designated compliance officer for guidance.

Low-Risk Customer Profiles

Customers considered low risk generally include:

- Individuals with stable income from verifiable sources (e.g., employment, pensions, state benefits)
- Individuals financially supported by a partner with a clear source of legitimate income

Enhanced Due Diligence for High-Risk Customers

For customers assessed as high risk, additional information must be collected to determine the legitimacy of their funds and wealth. This includes verifying:

- The origin of funds
- The customer's overall financial profile
- Supporting documentation to confirm lawful income and activities

Ongoing Business Risk Assessment

The Company conducts regular reviews of its **business-wide risk assessment** to ensure it remains current with:

- Changes in payment methods
- Market expansion or geographic diversification
- Introduction of new products or games
- Modifications in regulatory requirements

Transaction and Payment Method Risk

All payment types and financial interactions are evaluated to assess how they might facilitate money laundering or terrorist financing. This includes examining the structure, frequency, and nature of transactions.

Risk Categorization Framework

The Company classifies customer and transaction risk as **low**, **medium**, or **high** using the following factors:

- Transaction volume and size
- Complexity and transparency of customer behavior
- Geographic and sectoral vulnerabilities
- Effectiveness of internal controls

Assessment of Controls

Periodic assessments are conducted to evaluate the strength and adequacy of current controls, which include:

- KYC and identity verification systems
- Continuous transaction monitoring protocols
- Processes for identifying and reporting unusual activity
- Staff training initiatives
- Internal audits to detect control weaknesses or areas for improvement

Risk Mitigation Measures

The Company employs a range of mitigation strategies to address identified risks:

- Application of enhanced due diligence for high-risk clients and activities
- Use of AI-driven tools for proactive transaction monitoring
- Setting clear thresholds and alerts for unusual behavior
- Updating risk assessments in response to new threats or changes in operations
- Strengthening onboarding and monitoring standards
- Documenting control evaluations and risk mitigation efforts
- Developing standardized procedures for unusual activity reporting
- Prompt communication of ML/TF risks to relevant authorities
- Scheduling routine reviews of the overall risk framework
- Adapting controls based on new AML/CFT/CPF typologies or regulatory guidance
- Delivering continuous training on emerging risks and compliance expectations

6. Customer Risk Assessment (CRA)

The Company acknowledges that each client presents a unique level of risk based on their individual characteristics and behavior. To manage this effectively, a structured **Customer Risk Assessment (CRA) Framework** has been developed to evaluate and categorize clients according to their risk profile.

This framework enables the Company to assess both new and existing customers using a consistent set of risk indicators. Clients whose profiles raise potential concerns are flagged for **Enhanced Due Diligence (EDD)**, including increased transaction monitoring, or in some cases, refusal or termination of the business relationship.

The CRA serves as the basis for determining the appropriate level of **Customer Due Diligence (CDD)** to be applied and helps the Company identify customers who may pose a higher risk of **money laundering (ML)** or **terrorist financing (TF)**.

Key Risk Considerations in the CRA

In conducting the Customer Risk Assessment, the Company will take into account the risk factors outlined in Section 7, as well as other critical indicators, including but not limited to:

- **Customer Reputation:** The Company will assess whether the individual or entity has been associated with criminal activity, particularly financial crimes or terrorism, based on adverse media or regulatory findings.
- **Customer Conduct and Documentation:**
 - Reluctance or refusal to provide requested documentation or information without a valid reason
 - Submission of documentation that appears questionable in terms of authenticity or accuracy
 - Additional verification may be conducted using reliable, independent sources, including public databases and social media platforms, to validate customer identity and background

Methods of Customer Identification

The Company employs a range of verification techniques to ensure accurate identification of customers, including:

1. Standard Document Verification

Customers are required to submit valid identification documents, such as:

- A passport (photo and personal data page)
- A driver's license
- Additional supporting documents as specified in this AML Policy
Where necessary, further documentation may be requested to confirm the legitimacy of the customer's identity

2. Two-Factor Authentication (2FA)

Remote customer verification may be performed using **two-factor or multi-factor authentication (MFA)**.

- A verification code is sent to the customer's registered email address or mobile number
- The authentication process helps confirm the ownership of contact information and adds an extra layer of security

These identification methods are critical for detecting impersonation attempts and reducing the risk of onboarding individuals with fraudulent or unverifiable identities.

7. Customer Acceptance Policy

Introduction

The Company's general policy is not to accept any players whose funds have emanated from ill-gotten means, and to comply with all applicable obligations in relation to anti-money laundering (AML) and know your customer (KYC). The Company identifies all players prior to establishing a business relationship and proceeds to verify the data provided on certain activities being carried out, which may be first deposit, cumulative deposit thresholds being reached, cumulative withdrawal transactions exceeding XCG 4000 or reaching other triggers. For the purposes of converting XCG into Euros and vice versa, the Company uses the rate from xe.com. Players who are not registered will not be permitted to play for real money. One of the main drivers is to protect our operations from fraudulent transactions. The other key driver is preventing players from being able to launder money using our services; such money-laundering could take the form of either:

(a) a customer gambling using funds which they have obtained through criminal conduct – proceeds of crime; or

(b) a customer seeking to disguise the fact that they have obtained money from criminal conduct by passing it through our account in an attempt to 'clean' it.

It is important that the Company has a clear and concise understanding of all customer practices in order to avoid any possibility of money laundering and/or terrorist financing exposure. Every member of staff must be alert for the possibility that the Company's services could be used for money laundering purposes, or that in the course of their work they could become aware of criminal or terrorist property. If after gathering and considering routinely available information, the member of staff is entirely satisfied that reasonable grounds for suspicion are not present, no further action should be taken otherwise where there reasonable grounds for suspicion, the staff shall raise the matter with the responsible person. To this end, the Company restricts or prohibits the commencement of business relationships with customers and/or entering into transactions that fall outside our established risk appetite.

Age Verification

The Company will not accept any player under the age of 18 years (or other age specifically prescribed by law in certain targeted jurisdictions).

Countries and territories excluded for registration

Below is the general list of banned countries; however, it is not exhaustive and might also include other countries that may have been banned due to various reasons, e.g., change in FATF recommendations, countries banned by license agreements, countries with other deficiencies etc.

1. Afghanistan
2. Algeria
3. Angola
4. American Samoa
5. Aruba
6. Australia
7. Antigua and Barbuda
8. Bahamas
9. Barbados
10. Belize
11. Bermuda
12. Belgium
13. Bonaire
14. Bosnia and Herzegovina
15. Bolivia
16. Burma/Myanmar
17. Burundi
18. Burkina Faso
19. Bulgaria
20. Cameroon
21. Central African Republic

- 22.Curaçao
- 23.Côte d'Ivoire
- 24.China
- 25.Denmark
- 26.Democratic Republic of the Congo
- 27.Egypt
- 28.Eritrea
- 29.Estonia
- 30.France
- 31.French Guyana
- 32.Greenland
- 33.Guadeloupe
- 34.Guam
- 35.Guatemala
- 36.Haiti
- 37.Holy See (Vatican City)
- 38.Jamaica
- 39.Italy
- 40.Iran
- 41.Iraq
- 42.ISIL and Al-Qaida
- 43.Ivory Coast
- 44.Kenya
- 45.Lao People's Democratic Republic
- 46.Lebanon
- 47.Libya
- 48.Lithuania
- 49.Kuwait
- 50.Malaysia
- 51.Marshall Islands
- 52.Martinique
- 53.Maldives
- 54.Mali
- 55.Monaco
- 56.Mozambique
- 57.Namibia
- 58.Nepal
- 59.Netherlands
- 60.North Korea (Democratic People's Republic of Korea)
- 61.Occupied Palestinian Territory
- 62.Poland

63. Puerto Rico
64. Qatar
65. Reunion
66. Republic of Guinea
67. Saba
68. Saint Barthelemy
69. Saint Martin
70. Saint Pierre and Miquelon
71. Singapore
72. Spain
73. South Africa
74. Somalia
75. South Sudan
76. St. Eustatius
77. Sudan
78. Syria
79. Tunisia
80. Trinidad & Tobago
81. USA
82. US Minor Outlying Islands
83. Virgin Islands (UK)
84. Venezuela
85. Vietnam
86. Yemen
87. Zimbabwe

It is prohibited to use our services and play Gambling Games from Curacao, therefore, access to our Website is prohibited from Curacao.

The Company takes into account a variety of sources of information produced by the FATF and non-governmental well-known bodies, including:

- Countries on the FATF list of High Risk Jurisdictions subject to a Call for Action;
- Countries on the FATF list of Jurisdictions under Increased Monitoring;
- Countries on the CFATF Public Statement,
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT/CPF regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

The Company has created a list of countries that is used to outline high-risk, medium-risk and low-risk jurisdictions (APPENDIX 1).

The Company does not cooperate with clients (players) whose jurisdiction is included in the FATF black

and gray lists and other sanctions lists.

The following categories of players will not be accepted at registration/post-registration checks:

- Players residing in non-reputable or banned jurisdictions,
- IP login registered in a non-reputable or banned jurisdiction,
- Sanctioned individuals, Players under the age of 18.

However, on a case-by-case basis, the Company has the right to refuse any applicant for business or terminate an existing business relationship if the required Customer Due Diligence requirements are not satisfied. A departure from the above, may be applicable, on a case-to-case basis, following the approval of Senior Management.

Accepted payment methods

Certain payment methods must be treated as high risk factors, this includes:

- Cash;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- The use by customer of cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Types of financial services (credit/marker, currency exchange, check cashing);
- Using cash to fund a pre-paid card poses similar risks as cash;
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also. e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the online casino. This may be useful for dishonest customers who wish to disguise their gambling.
- Other payment methods that may not leave or disrupt the audit trail and allow the customer to operate with a degree of or complete anonymity such virtual currencies.

The Company shall only engage with payment service providers, including banks, e-wallets, and cryptocurrency processors, that are duly licensed and supervised by a competent financial authority in their jurisdiction. All payment methods used must comply with applicable laws and regulatory requirements of **Curaçao**, as well as international standards on anti-money laundering and counter-terrorist financing and proliferation financing (AML/CFT/CPF). The Company will conduct appropriate due diligence to ensure that all payment providers maintain effective compliance frameworks and are not located in high-risk or non-cooperative jurisdictions as identified by recognized international bodies.

The Company will always keep track of transactions carried out using these payment methods and identify funds that are received or remitted by customers.

No cash policy

The Company does not accept cash deposits nor will cash withdrawals be processed.

High-risk products and services

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others.

High risk products and services include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;

- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.B. roulette, craps -> even bets);
- Peer to peer gaming;
- The use by customer of accounts held or cards issued in the name of third parties;
- Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Games involving multiple operators (Poker on platforms shared by multiple operators);

8. Customer Due Diligence

The Company implements a three-tiered approach to customer due diligence, which includes:

- **Simplified Due Diligence (SDD)**
- **Regular Due Diligence (RDD)**
- **Enhanced Due Diligence (EDD)**

Each level is applied based on the assessed risk associated with the customer's profile and activity.

8.1. Simplified due diligence (SDD)

Simplified Due Diligence (SDD) serves as the initial phase within the Company's risk-based approach. It is applied during the period between customer registration and the first deposit, specifically for individuals originating from jurisdictions classified as low risk.

Simplified due diligence is performed by the customer providing identification details prior to registration. Upon registration, customers have to indicate their residence country and validate their e- mail address, after which they shall fill in the following personal details:

- full name;
- permanent residential address;
- date of birth;
- place of birth;
- nationality;
- identity number.

However, in low risk scenarios identification may be limited to three personal details:

- full name;
- permanent residential address;
- date of birth;

In high-risk scenarios, the Company may determine that collecting additional personal information is necessary to adequately mitigate the elevated risk of money laundering or terrorist financing.

As a matter of policy, no customer is permitted to deposit or withdraw funds until the registration process has been fully completed.

During this phase, all customers are screened using verification tools that include checks against sanctions lists, Politically Exposed Persons (PEP) databases, and adverse media sources. Individuals flagged through these screenings—particularly those under sanctions—will not be accepted as customers.

- The following categories of players will not be accepted at registration/post-registration checks:
- Players residing in non-reputable or banned jurisdictions,
- IP login registered in a non-reputable or prohibited jurisdiction,
- Sanctioned individuals – subject to additional Sanctions list and PEP (politically exposed person) checks. Due to their influence, PEPs are more likely to be involved in aiding or abetting money laundering, racketeering, and financial fraud. As such, working with PEPs entails certain risks for financial institutions and other entities. Since there is no universal definition of PEP, most countries refer to the one provided by Financial Action Task Force:
 - A present or past senior government official;
 - Prominent politicians belonging to a certain party;
 - An executive of a governmental commercial enterprise formed for the benefit of a government official;
 - Close family members of a government official;
 - publicly-known associate of a financial institution.
 - Transactions involved with PEPs are considered as high-risk transactions.

In line with the Company's risk-based approach, all reasonable measures will be taken to verify the true identity of customers. This process includes reviewing and validating the information provided to ensure it is accurate, consistent, and free from logical inconsistencies.

Where appropriate, official documents will be used to confirm a customer's identity. However, in light of the growing threat of identity fraud, the Company may also apply non-documentary verification methods when necessary. If doubts remain regarding a customer's identity, these alternative methods may be employed to further support the verification process.

The evaluation will focus on whether key personal details—such as name, residential address, date of birth, and identification numbers—are coherent and verifiable, thereby allowing the Company to reasonably confirm the customer's true identity.

Although the Company is not legally obligated to authenticate the documents submitted by customers, government-issued identification may be used as a reliable basis for identity verification. However, if any clear indications of fraud are detected in the documentation, these concerns must be considered when assessing whether the customer's identity can be confidently verified.

The verification process will be completed within a reasonable timeframe and must be finalized before a customer account is activated. Depending on the nature of the account or transaction, the Company reserves the right to delay or restrict transactions until verification is complete. If extended verification is required, certain transaction types or amounts may be temporarily limited.

Should any information arise that raises suspicion of money laundering, terrorist financing, or other illicit activity, the matter will be escalated to the AML Compliance Officer. Where appropriate, a Unusual Transaction Report (UTR) will be submitted in accordance with applicable regulatory requirements.

The Company may engage qualified third-party service providers to perform elements of the Customer Due Diligence (CDD) process, provided that appropriate confidentiality agreements are in place to safeguard

customer information.

CDD will remain ongoing until all required documentation and information, as specified in this Policy, have been successfully collected and verified. If a customer fails or refuses to provide the necessary materials within two weeks of the initial request, the matter will be flagged by the AML specialist as potentially unusual, and appropriate measures will be taken in accordance with the Company's AML/CFT/CPF procedures.

Where the initial risk assessment indicates no material concerns, **Simplified Due Diligence (SDD)** may be applied. SDD entails a basic level of identity verification and is reserved for clients assessed to pose a **very low risk** of money laundering, terrorist financing, or related financial crimes.

Eligibility for SDD is determined through an initial risk evaluation, considering variables such as the customer's industry, geographic location, financial behavior, and transaction transparency. This approach is most appropriate for customers with a clear and verifiable financial background, where further verification would not substantially improve risk mitigation.

Simplified Due Diligence (SDD) may only be applied to customers who have been formally assessed and documented as low-risk. Typically, this includes individuals with a single, easily verifiable source of income originating from a regulated jurisdiction. Under no circumstances may SDD be used if there is any indication or suspicion of money laundering, terrorist financing, or related criminal activity—even if the customer's initial risk profile appears low.

All Company personnel, including employees, directors, and officers, are strictly prohibited from disclosing whether a customer has been reported to the **Financial Intelligence Unit (FIU)**. Performing CDD in the presence of suspected illicit activity poses a risk of **tipping-off**, which may alert the customer and compromise regulatory investigations. If it is reasonably believed that continuing with the CDD process may reveal that a report is being filed, the Company should suspend the process and instead proceed directly with filing a report with the FIU.

Verification procedures are designed to ensure that the individual is who they claim to be. This includes evaluating the **quality, legibility, and authenticity** of submitted documents. Special attention must be paid to potential indicators of fraud or forgery, and if documents originate from foreign or unfamiliar sources, additional care should be taken to validate their legitimacy.

8.2. Regular due diligence

The Regular Due Diligence process is triggered on the occurrence of one of the following events:

- Single/Cumulative withdrawals exceeding €2200 or the equivalent of XCG 4 000 in currency available on the Website or reaching other triggers;
- Attempt to request a name change (clients cannot do so automatically).

In order to verify the details on their account, the customer is required to send customer care a photocopy or scan of one document from each of the categories listed below:

Personal Identification - one photo ID from the following list:

- 1) Current Signed passport
- 2) Current photo-card Driver's License (Provisional or Full)
- 3) Current Full Driver's License (old style paper version)
- 4) Current EU National Identify Card
- 5) Other recognized identity card such as an Armed Forces Identity Card

Address Verification - one of the following:

- 1) Utility bill (within last 3 months)
- 2) Current photo-card Driver's License (Provisional or Full) (Applies for UK DL's)
- 3) Current Full Driver's License (old style paper version)
- 4) ID card with address + Passport or additional ID
- 5) Bank/Credit Union/Building Society/Credit Card statement or passbook (within last 3 months)
- 6) Council tax bill or payment book (within last 3 months)
- 7) Recent mortgage statement (within last 3 months)
- 8) Current local council rent card or tenancy agreement (private tenancy agreements are not acceptable)
- 9) Home Insurance certificate or policy
- 10) Motor Insurance certificate or policy
- 11) Electoral roll
- 12) Credit reference agency
- 13) Mobile bills are not accepted

Source of Payment Verification/Proof of Payment - one of the following:

- 1) Company account registered Credit or Debit card
- 2) Copy of Credit or Debit card account statement of a card registered on with Company account (less than 3 months old)
- 3) Copy of bank statement - must have Company transaction or card number visible on it (less than 3 months old)

When requesting such documentation, the customer must always be informed that:

- The card number must be blanked out leaving only the first 6 and the last 4 digits visible together with the expiry date.
- The documents must be clear and legible.
- The documents should show the residential address.

8.3. Enhanced due diligence

Enhanced due diligence (EDD) checks of the customer may be initiated resulting from hits on Sanctions and PEP-lists, and through various financial or behavioral triggers, including but not limited to:

- Withdrawal amount;
- Depositing/withdrawing behaviour and pattern;
- Data mismatching;
- Gameplay behaviour;
- Combination of the above.
- When the Company receives previously undisclosed information regarding the Customer's source of funds or source of wealth.
- Upon identifying a Customer or prospective Customer as a Politically Exposed Person (PEP), or as a family member or close associate of a PEP. In such cases, prior to establishing a business relationship, written approval must be obtained from the Managing Director. The Compliance Officer must submit a request for approval within five (5) business days of identifying the PEP status. The Managing Director is required to respond with an official approval or rejection within five (5) business days of receipt. An annual review of all such relationships must be conducted to

reassess risk and ensure adherence to enhanced due diligence measures.

- If the Customer presents unusual identification documents that are unverifiable or inconsistent with other information previously provided or publicly available.
- When a case is identified internally or reported by the GCB as high-risk for money laundering or terrorist financing.
- When dealing with a Customer located in a high-risk third country, or in any transaction where one of the parties is based in such a jurisdiction.
- If it is discovered that a Customer has submitted false or stolen identity documents or information, and the Company intends to continue the relationship.
- When transactions are unusually large, complex, or follow an atypical pattern without a clear economic or legal rationale.
- In any other scenario that inherently poses a heightened risk of money laundering or terrorist financing.
- If the Customer refuses to disclose the legitimate source of funds, or if the information provided is false, misleading, or materially inaccurate.
- When the Customer is located in, transacting with, or operating in jurisdictions considered high-risk due to secrecy laws, tax evasion concerns, narcotics trade, insufficient AML/CFT/CPF frameworks, or ongoing conflict or terrorism threats.
- When the Customer is unable to clearly explain the nature of their business or demonstrates limited understanding of their industry.
- When the Customer's legal or mailing address is linked to multiple unrelated accounts or entities.
- If the Customer appears to act on behalf of an undisclosed principal and is unwilling to share relevant information.
- If the Customer's background or profile is inconsistent with the expected behavior for their declared business activities.
- If the Customer derives wealth from high-risk industries—such as cryptocurrency, gambling, financial services, weapons manufacturing—or cannot adequately explain their source of wealth.
- If the Customer uses high-risk payment methods, including but not limited to:
 - a) Cryptocurrency transactions
 - b) Payments from shell banks
 - c) Transactions through banks operating in high-risk jurisdictions
 - d) Use of third-party credit/debit cards
 - e) Unauthorized or excessive transactions
- If the Customer appears to be acting on behalf of another party or an unidentified beneficial owner.

Documentation Required During Enhanced Due Diligence

During the EDD process, the Company is authorized to request the following from individual clients:

- Written explanations regarding the source of funds or source of wealth, along with supporting documentation.
- Written statements describing the client's financial capacity and employment or income source.
- Any documentation that supports the written declarations.
- Additional information about the intended nature and scope of the business relationship.
- Clarification on the purpose behind specific transactions.

Record Maintenance and Review

The Company is authorized to ensure that all documents, data, and information collected through the Customer Due Diligence process remain current and relevant. This includes conducting periodic reviews, particularly for high-risk customers.

Key Components of the Customer Due Diligence (CDD) Process

- **Identification:**

The CDD process begins with identifying and documenting potential risks related to money laundering or terrorist financing. These risks may stem from known typologies, industry alerts, or emerging vulnerabilities within the customer's profile or transaction behavior.

- **Risk Analysis:**

Once identified, each risk is assessed in terms of its nature, origin, likelihood of occurrence, and potential impact. This step enables the Company to gain a contextual understanding of the threat and assign it an appropriate risk rating.

- **Risk Evaluation:**

Evaluated risks are prioritized based on their severity and relevance. This prioritization guides the development and application of suitable risk mitigation strategies, ensuring that the Company allocates resources effectively.

- **Risk Categorization and Proportional Measures:**

Customers and transactions are classified into risk categories—such as low, medium, or high—based on the assessment. This allows the Company to implement proportionate due diligence measures and ongoing monitoring aligned with each risk level.

- **Additional Verification Measures:**

To enhance the reliability of the CDD process, the Company may use supplementary verification tools and third-party data sources. These measures may include in-depth reviews of the customer's background, ownership structures, financial history, and alignment of transaction patterns with the declared purpose of the relationship.

EDD for Complex or Unusual Transactions

For transactions that are unusually large, complex, or lack a clear purpose, the following EDD measures must be undertaken:

- Investigate the background, purpose, and economic rationale behind the transaction and overall client relationship.
- Increase the level and frequency of monitoring related to the business relationship to identify unusual patterns.
- Engage third-party service providers, if necessary, to support enhanced monitoring—subject to confidentiality agreements.

EDD Completion and Follow-Up

EDD must be finalized once all required documentation and information have been received from the customer. If the customer fails or refuses to provide the requested materials within **14 days** of the initial request, the AML specialist must record the matter as **unusual** and initiate the appropriate escalation steps in accordance with this Policy.

During the broader CDD process, customers may continue to access their gaming accounts. However, if the **EUR 2,200 threshold** (or **XCG 4,000 equivalent**) is reached, the customer will be **prohibited from depositing or withdrawing funds** until the necessary verification steps are completed.

If the required documents and information are not submitted within **30 days** from the point the threshold is met, the Company is obligated to **terminate the business relationship** and **report the transaction to the Financial Intelligence Unit (FIU)**.

These measures are essential to ensure compliance with AML/CFT/CPF regulations and to prevent the continuation of services in the presence of unresolved or potentially unusual circumstances.

In case the obligations arising from the customer due diligence cannot be met, the Company cannot establish the business relation or perform the transaction or is obliged to terminate the business relationship with the player. The Company may decide to either close the account or to keep it blocked and suspended in its entirety.

In the event that the player makes the requested information and/or documentation available to the Company following the closure or the suspension and blocking of the gaming account, the Company has

to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

Where there is no reason for the retention of funds, the funds are to be remitted back to the player. This has to be done through the same channels used to receive the funds.

9. Ongoing Monitoring

Once a business relationship is established, the Company is required to perform ongoing monitoring in compliance with the **National Ordinance for Identification when Rendering Services (NOIS)**, and the **National Ordinance Reporting Unusual Transactions (NORUT)**.

This ongoing monitoring process comprises two essential components:

A) Scrutiny and monitoring of transactions:

The Company will continuously monitor transactions throughout the duration of the business relationship to ensure they align with the customer's typical behavior and assessed risk profile.

This monitoring may occur in real time before transactions are executed (**pre-transaction monitoring**) and/or retrospectively after transactions have taken place (**post-transaction monitoring**).

Where participants are flagged with a notification after the account opening, accounts are locked until customer due diligence procedures are in place. Some of the possible notifications that can be triggered are:

- SIPs, Watchlist;
- A client residing or located in a country, the AML/CTF/CPF credentials about which the Company has doubts;
- A client who has been the subject of a disclosure;
- A client flagged on the sanctions list;
- A client depositing gambling/withdrawing big amounts;
- A client flagged as a fraudster.
- To mitigate risk, all payments and fraud teams are instructed to flag any instances where a customer uses a payment card registered to a third party—that is, when the cardholder's name differs from the customer's registered information. In such cases, the account will be blocked, and the customer will be required to provide an explanation along with supporting documentation.
The following transactions or intended transactions are deemed unusual:
- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- Transactions in the amount of XCG 5000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means.
- This includes but is not limited to:
- A cashless transaction in the amount of XCG 5000 or more.
- A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the player.
- Accepting or releasing a deposit in the amount of XCG 5000 or more at the request of the player;
- Sale to a player of chips in the amount of XCG 5000 or more. "Chips" include but is not limited to tokens and credits.
- A cash out in the amount of XCG 5000 or more;
- A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of XCG 5000.
- Presumed money laundering transactions or terrorist financing: Transactions where there is cause

to presume that they can be related to money laundering or terrorist financing. The Company is registered with the FIU and has access to goAML reporting portal.

B) Update the information and the documents of the clients:

The Company requests fresh identification documents when the expiry date of identification documents held on file is reached. This can be done on a risk-sensitive basis or be linked to specific trigger events.

Below is a non-exhaustive list of trigger events initiating a player review.

- High deposits/withdrawals;
- Unusual gameplay activity;
- Non-wagering of funds;
- Mismatch in data (indicated data and/or digital fingerprint data);
- Potential 3rd party usage;
- Potential minor usage;
- Links to other customers.
- Possible hits on screening of Sanctions and PEP-lists.

If the Company is unable to satisfy the player due diligence requirements, it must either refrain from establishing the business relationship or terminate any existing relationship. All attempts to obtain the necessary information and documentation must be thoroughly documented.

Following this, the Company may opt to either close the player's account or maintain it in a fully blocked and suspended state. Should the player later provide the required information or documents after account closure or suspension, the Company is obligated to reassess whether the delay affects the money laundering or terrorist financing risk associated with that business relationship.

The Company must assess whether there are any indications of money laundering, terrorist financing, or fraud. However, a player's hesitation or refusal to provide due diligence information should not be automatically interpreted as unusual. Instead, the Company should consider all relevant factors and available information to determine whether reasonable grounds for suspicion exist. If such suspicion arises, the Company is obligated to report the unusual transaction to the Financial Intelligence Unit (FIU).

If there is no reason to retain the funds, they should be returned to the player through the same channels used to receive them.

The risk-based supervision process consists of two main components:

- 1) Identifying and understanding risks, and
- 2) Mitigating those risks.

A risk analysis must be performed to determine where the money laundering and terrorist financing risks are the greatest. It is important to identify higher risk customers, products and services, including delivery channels, and geographical locations. These are not static assessments. They will change over time, depending on how circumstances develop, and how threats evolve.

The strategies to manage and mitigate the identified money laundering and terrorist financing risks are aimed at preventing the activity from occurring through a mixture of deterrence (e.g. appropriate CDD measures), detection (e.g. monitoring and unusual transaction reporting), and recordkeeping so as to facilitate investigations.

To identify and understand the risks, the responsible person shall check the Client according to the Mandatory check list:

Category	Mandatory check list
----------	----------------------

Geographic	High-Risk Jurisdiction according to FATF (high risk of ML/AT)	Jurisdiction where gambling is forbidden	Excluded Jurisdiction according to the Terms and conditions	Jurisdiction that provides for special gambling requirements (age/ welfare etc.)	Jurisdiction without gambling regulation	Multi-jurisdiction / IP addresses
Transaction	Use of debit or credit cards that do not belong to the customer	Funds from offshore bank or bank in the High-Risk Jurisdiction	Payment that is impossible to authorize	Unusual or huge amount	Fractionation of payments	Use of new (uncommon) debit or credit cards
Documents	Contain signs of forgery	Are insufficient to identify the person	Do not belong to the client	Proof the risks specified in this table	Out of date	1 month or less before expiration
Customer	PEP	Most wanted person	Self-excluded or excluded from gambling	Recognized as undesirable (black list)	Does not meet the requirements set out in Terms and conditions	Minimizes communication with the authorized person

Enhanced DD	Unknown source of funds	Fail to provide mandatory information	Information is not satisfied or insufficient	Fail to pass video call	Conflicting information	Avoidance of enhanced DD
-------------	-------------------------	---------------------------------------	--	-------------------------	-------------------------	--------------------------

The Client shall be categorized as high risk in case of at least one red zone.

The Client shall be categorized as medium risk in case of at least one yellow zone.

The Client shall be categorized as low risk in case of absence of yellow or red zones.

After identification and understanding the risks, the responsible person should choose the following measures (at least one):

Red zone	Enhanced and Ongoing DD	Block of the account	Freeze of all transactions	Withdraw from the business relations	Notify the relevant authorities
Yellow zone	Enhanced DD	Ongoing DD	Temporarily suspend the game account/ transactions	Video call	Additional documents
Green zone	Ongoing DD	Video call	Additional documents	Additional explanations	Photo with ID documents

The principle of chosen measures should be directed in accordance with priorities so that the greatest risks receive the highest attention. The alternative approaches are that resources are either applied evenly, or that resources are targeted, but on the basis of factors other than risk.

An effective risk-based approach shall allow to exercise reasonable business and professional judgement with respect to customers. Application of a reasoned and well-articulated risk-based approach shall justify the judgements made with regard to managing potential money laundering and terrorist financing risks.

Performing of the Due Diligence shall be done in the following terms:

	Additional check	Ongoing DD	Enhanced DD
Red zone	Always on every risk	Always	Always
Yellow zone	In case of 1 yellow zone – one request	In case of more than 2 yellow zones – until they are eliminated	In case of more than 3 yellow zones – until they are eliminated
Green zone	one request per month (in case of unusual activities)	in case of unusual activities (close to yellow zone)	in case of unusual activities (close to red zone)

10. Reliance on Third Parties for Customer Due Diligence

The Company may delegate specific components of the Customer Due Diligence (CDD) process to third-party providers, provided that all conditions outlined in this Policy are met. Any third party engaged must be subject to CDD and record-keeping obligations equivalent to those imposed on the Company. Furthermore, the third party must maintain an independent, pre-existing business relationship with the customer that is distinct from the relationship being established with the Company.

While delegation of CDD tasks is permitted, the Company retains full accountability for ensuring that all CDD requirements are effectively implemented. A formal agreement must be established with the third party, mandating that all relevant identification data and supporting documentation be accessible upon request. This arrangement should be subject to regular review and testing to verify its continued compliance and effectiveness.

Notwithstanding reliance on third parties for certain CDD activities, the Company remains solely responsible for conducting its own customer risk assessments, identifying Politically Exposed Persons (PEPs), and executing ongoing monitoring throughout the duration of the business relationship.

11. Risk profiles

Adoption of a Risk-Based Approach

Our Company employs a Risk-Based Approach (RBA) to Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and counter-proliferation financing efforts. This approach ensures that the measures taken to prevent or mitigate associated risks are proportionate to the level of risk identified. Accordingly, higher-risk situations require enhanced due diligence and stronger controls, while lower-risk scenarios may allow for simplified measures, provided they are consistent with the overall risk environment, particularly in relation to terrorist financing.

Use of Customer Data for Profiling

The Company may utilize internally collected data over time to develop a profile of a typical customer. This method is applicable only when the Company has a sufficiently large and diverse customer base to produce statistically valid average profiles.

Application of the Risk-Based Approach

In implementing the Risk-Based Approach, the Company shall:

- Conduct prior risk assessments to evaluate the likelihood of money laundering or terrorist financing occurring within its operations;
- Develop and enforce appropriate policies, procedures, and controls designed to address and mitigate identified risks;
- Continuously monitor the effectiveness of these policies and procedures and make improvements as necessary.

Documentation of Risk Assessments

The Company shall document all risk assessments, including the rationale for actions taken. Risk identification will consider the following categories:

- (i) Country or geographic risk;
- (ii) Customer risk;
- (iii) Transaction risk;
- (iv) Product and service risk;
- (v) Delivery channel risk.

Country and Geographic Risk

Certain countries inherently pose higher risks for money laundering and terrorist financing. In addition to internal insights, the Company may rely on external credible sources to identify countries presenting elevated risk. These include reports from the Financial Action Task Force (FATF) and other reputable non-governmental organizations that monitor corruption and financial crime risks. Customers associated with high-risk jurisdictions—whether by nationality, place of business, or residence—may present elevated AML/CTF/CPF risks. The Company’s staff may verify customer location details to mitigate additional risks linked to cross-border transactions. Country risk should also be assessed in combination with customer-specific risk factors.

Geographical Risk Considerations

Geographical risk encompasses the risks arising from the customer's nationality, country of residence, place of birth, and the source of their wealth. Factors increasing geographical risk include jurisdictions with weak AML/CTF/CPF frameworks, high levels of corruption, international sanctions, or known terrorist activity. The Company will consult a range of authoritative sources, such as:

- FATF list of High-Risk Jurisdictions subject to a Call for Action;
- FATF list of Jurisdictions under Increased Monitoring;
- CFATF Public Statements;
- U.S. Department of State’s International Narcotics Control Strategy Report (INCSR);
- European Commission list of third countries with strategic AML/CFT/CPF deficiencies;
- Sanctions lists published by the Office of Foreign Assets Control (OFAC);
- Credible sources identifying jurisdictions supporting terrorism or hosting terrorist organizations;
- Transparency International’s Corruption Perception Index.

High-Risk and Low-Risk Country Lists

The Company maintains an up-to-date list of countries categorized as high or low risk. This list is available in the Company’s Website Policy and is reviewed and updated regularly to reflect emerging threats and regulatory guidance.

Industry-Specific Risk Indicators

The Company also considers red flags unique to the online gambling sector, including but not limited to:

- Frequent changes in betting behavior or use of multiple accounts to avoid detection;
 - Deposit activity followed by minimal gambling and rapid withdrawals;
 - Collusive practices, such as "chip dumping," particularly in peer-to-peer games.
-

12. Cryptocurrency

Virtual Assets and Cryptocurrencies

Customers engaging in deposits or withdrawals using cryptocurrencies shall be subject to Enhanced Due Diligence (EDD). This includes, where feasible, verification of the source of funds through blockchain analysis.

The Company will actively monitor for unusual behavior—such as rapid conversion of cryptocurrencies to fiat currency with limited gambling activity—and will report any such transactions to the Financial Intelligence Unit (FIU) in accordance with regulatory obligations.

13. Compliance and consequences of non-compliance: Termination of business relationship and asset freeze

Business Relationship Termination

To avoid involvement in potential money laundering offenses, the Company reserves the right to terminate its relationship with a customer under the following circumstances:

- If it is known that the customer is attempting to use gambling services to launder illicit funds or to engage in criminal spending.
- If the assessed risk of breaching the Proceeds of Crime Act (POCA) is deemed unacceptably high.
- If the customer's gambling behavior raises increasing suspicion or reveals actual evidence of money laundering.
- If the customer is reasonably believed not to be the individual they claim to be.
- If the Company is unable to carry out the required Customer Due Diligence (CDD) measures.
- If the customer fails to provide the requested documentation within 30 days after reaching the equivalent of the XCG 4,000 threshold.

Mandatory Reporting and Fund Management

The Company will terminate the relationship and report to the FIU when there are grounds to suspect money laundering or terrorist financing. If no such suspicion exists, funds will be returned to the original bank account or wallet from which they were received. In cases where suspicion is present, the Company's internal procedures will determine whether the funds should be frozen. Caution must be exercised to avoid tipping off the customer when taking such actions.

Sanctions Compliance

The purpose of the Company's sanctions compliance framework is to:

- Prevent the misuse of the Company's services for sanctionable activities;

- Identify and block the assets of designated individuals, entities, or jurisdictions;
- Ensure the Company's full compliance with:
 - The **Sanctions National Ordinance of Curaçao**
 - The **Kingdom Sanction Law (Rijkswet Financiële Sancties)**
 - **UN Sanctions Regimes**
 - **EU Restrictive Measures**
 - **Other applicable international sanctions regimes**

This framework applies to all business units, employees, customers, and third-party relationships across all jurisdictions in which the Company operates.

List-Based Screening and Monitoring

The Company implements robust **name and entity screening procedures**, conducted through automated compliance tools integrated with up-to-date global sanctions databases.

- **Screened parties include:**
 - All customers and beneficial owners (natural and legal persons);
 - Corporate officers and controlling persons of legal entities;
 - Agents, introducers, and other third-party intermediaries;
 - Transaction counterparties, wallet addresses, and relevant IP data.
- **Screening is conducted:**
 - **At onboarding (initial due diligence);**
 - **Daily, as part of ongoing monitoring;**
 - **Immediately following updates to sanctions lists.**

Sanctions lists incorporated include but are not limited to:

- United Nations Consolidated Sanctions List;
- European Union Consolidated List of Financial Sanctions;
- Kingdom of the Netherlands designated sanctions lists;
- Other applicable national or international sanctions sources as determined by risk-based assessment.

Positive Match Protocol and Asset Freezing Measures

Where a match is identified and confirmed against a sanctions list, the Company shall immediately:

- **Block or freeze all funds and other assets associated with the designated subject;**
- **Prohibit any transaction, service, or economic resource from being made available;**
- **Refrain from notifying the customer or third party (no tipping-off);**
- **Report the finding without delay to the appropriate authorities, including:**
 - The **Financial Intelligence Unit of Curaçao (FIU Curaçao);**

- Any other competent regulatory or law enforcement body as required.

All asset freezing actions will be conducted in strict accordance with procedures set out in the Sanctions National Ordinance and in cooperation with the relevant supervisory bodies.

Governance, Training, and Controls

The Company maintains comprehensive internal controls to support sanctions compliance, including:

- Appointment of a qualified **Compliance Officer** responsible for sanctions oversight, escalation protocols, and liaising with authorities;
- Implementation of **segregated duties and system-based alerts** to prevent unauthorized overrides;
- Ongoing **employee training programs** tailored to sanctions obligations, with periodic refresher courses and role-specific modules;
- Maintenance of an auditable **sanctions register**, recording all screening results, alerts, internal investigations, freezing actions, and reports filed;
- Retention of all sanctions-related records for a minimum of **five (5) years**, or longer if required by law or pending investigation.

Risk-Based Application and Third-Party Oversight

The Company applies a **risk-based approach** to sanctions compliance, which includes:

- Enhanced scrutiny of high-risk jurisdictions, politically exposed persons (PEPs), and cross-border transactions;
- Due diligence on third-party service providers, affiliates, and payment processors to ensure **no indirect exposure to sanctioned persons or entities**;
- Reassessment of risk profiles whenever there are material changes to customer behavior, ownership structure, or relevant global sanctions regimes.

Handling of Funds Upon Termination

In cases where the relationship is terminated due to suspected money laundering or terrorist financing, customer funds shall be frozen and the FIU consulted before any further action. Where no suspicion exists, and following a satisfactory risk assessment, funds will be returned to the originating account within 14 calendar days.

14. Beneficial Ownership and Third-Party Verification

To ensure full compliance with the requirements of the **National Ordinance on the Identification of Clients (NOIS)** and the **National Ordinance on the Reporting of Unusual Transactions (NORUT)**, the Company has implemented robust procedures to identify and verify beneficial ownership and prevent undisclosed third-party involvement.

Identification and Verification of Beneficial Ownership

The Company defines a **beneficial owner** as any natural person who ultimately owns or controls a customer, or the person on whose behalf a transaction is conducted. This includes:

- Natural persons owning or controlling **25% or more of a legal entity** (directly or indirectly);

- Individuals exercising **effective control** over the entity through other means;
- The **settlor, trustee, and beneficiaries** in the case of trusts or similar legal arrangements.

Procedures:

- The Company requires all beneficial owners to provide a **beneficial ownership declaration**, supported by corporate documentation (e.g., shareholder registry, organizational chart).
- Identification documents of all beneficial owners are verified through independent and reliable sources.
- Enhanced due diligence (EDD) is applied where:
 - Ownership is layered or complex;
 - There is a **legal arrangement (e.g., trust, foundation)**;
 - Beneficial owners are high-risk or politically exposed persons (PEPs).

Beneficial ownership data is retained for a minimum of **five years** and updated regularly, particularly when material changes occur.

Prohibition of Undisclosed Third-Party Activity

The Company strictly prohibits customers from using its platform or services **on behalf of any third party** unless explicitly authorized and verified in accordance with applicable laws.

Customer Due Diligence Measures:

- During onboarding, customers are required to confirm that they are acting **on their own behalf**;
- Where there is any indication that a player may be acting for another party (e.g., unusual patterns, proxy access, shared IPs/devices), the Company conducts:
 - Additional source of funds/source of wealth verification;
 - Manual review of transactional behavior;
 - Possible account suspension pending clarification.

Third-party relationships are only permitted in exceptional, pre-approved cases, and only after full due diligence is conducted on both the primary customer and the represented party.

Ongoing Monitoring and Enforcement

- The Company continuously monitors transactions and behavior to detect possible **third-party involvement or changes in beneficial ownership**;
- Non-disclosure or misrepresentation of beneficial ownership or third-party status will lead to **account termination, asset freezing**, and, where appropriate, **filing of an Unusual Transaction Report (UTR)** to FIU Curaçao.

15. Reporting Procedures and Obligations

a. Internal Reporting Procedures

By employing the procedures as described in this policy and the Anti-Fraud and AML/CTF/CPF System (the System) fully investigating any transaction, we can identify unusual transactions or activities that could

be construed as money laundering or terrorist financing.’

There is an obligation for all staff members to report suspicions of money laundering or terrorist financing, and all suspicions should be reported immediately to the responsible department by completing the Internal Reporting Form.

These reports must be made by the Company’s employees when they have a suspicion in relation to a customer’s behavior or when they receive an alert from the System based on any transactions that matches the reporting threshold. In the latter case, before submitting a report to the responsible department, the employee must check whether the alert is simply a false positive.

Internal reports are to be submitted in writing using the standard template together with all relevant information and documentation available to the employee to assist the responsible department in making a determination as to how best to proceed.

The report must also include details on the customer who is the subject of concern and as full a statement as possible of the information giving rise to the knowledge or suspicion.

Where the report is based on the objective indicators, as outlined by pertinent Curacao legislation, such reports shall be submitted to the FIU within 48 hours of the transaction taking place.

Where the report is based on the subjective indicators, as outlined by pertinent Curacao legislation, such reports shall follow the timeline below:

- Internal Unusual Transaction Report (UTR) must be submitted to the Money Laundering Reporting Officer (MLRO) within 24 hours of the transaction taking place
- MLRO must make a determination as to the reportability of the transactions within 10 working days
- If the MLRO determines that the transaction and/or behaviour is indicative of ML/TF, the MLRO must submit the report to the FIU within 48 hours of making that determination.

The Company has appointed a Money Laundering Reporting Officer (MLRO) who is responsible for the reporting of unusual transactions to the Curacao FIU, as well as other transactions as per guidelines of the local FIU. In addition the Company has also enlisted the services of a compliance officer, whose tasks involve but are not limited to:

- manage the Customer Due Diligence;
- review of identification documents and information provided by the players at onboarding;
- consulting relevant watch and sanctions-lists;
- conducting further checks where necessary;
- develop and implement an in-house AML training program;
- managing and ensuring that transaction monitoring on players is conducted;
- analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions; and
- report any unusual transactions or activities to the MLRO.

The Money Laundering Reporting Officer (MLRO) must consider, without delay, every internal report

received to determine whether or not the information contained in the report: (a) does give rise to a knowledge or suspicion of ML/TF; or (b) whether additional information is necessary to reach this determination.

The responsibilities of the MLRO include but are not limited to:

- Keep records of internally and externally reported unusual transactions;
- Decide whether sufficient suspicion is required to generate reports on money laundering and adequately disclose it to the relevant authorities;
- Verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing; and
- Remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements;

Both the MLRO and the compliance officer shall maintain direct lines of communication with senior management to ensure accountability and transparency, as necessary and with respect to the relevant field of responsibility. Regular report on the status of the AML program, including identified risks, compliance issues, and corrective actions are provided to the Board of Directors and the CEO. The compliance officer collaborates with other departments, as needed, to ensure a comprehensive approach to compliance.

b. External reporting procedures

After considering the internal report and all the necessary documentation, when MLRO determines that there is:

(a) knowledge;

(b) suspicion; or

(c) reasonable grounds to suspect that:

- a transaction may be related to ML/TF (regardless of the amount involved); or
- a person may have been, is or may be connected with ML/TF; or
- ML/TF has been, is being or may be committed or attempted;

(a) Transaction amounts surpassing the respective thresholds as indicated by the objective indicators. The MLRO shall file a STR to FIU Curaçao and determines if reporting should also be done to other FIU in the country of an Outsourcing Provider.¹

The MLRO will not disclose the name of the employee who made the internal report to the FIU, and in completing this report MLRO must provide as much detail as possible together with the relevant identification and other supporting documentation.

The decision to file or not to file an unusual transaction report will always be at the discretion of the MLRO, and MLRO will not be subject to the direction or approval of other parties within the organization, provided that in reaching the decision on whether to file a report, MLRO may seek assistance from other employees of the Company or external advisors.

What are the Responsibilities of Compliance Officer?

- Decide whether sufficient suspicion is required to generate reports on money laundering and adequately disclose it to the relevant authorities.
- Verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- Risk assessment; One of the most sublime duties is to assume and manage various levels of risk. Managing, shaping, and reporting these risks. At this stage, the management needs to guide and give the necessary permissions.
- Observe and plan new legislation to develop AML policies, systems, and procedures to ensure effective implementation.
- Money laundering, terrorist financing, proliferation financing (AML/CTF/CPF), and fraud prevention are also under their responsibility.
- Ensure its customers know and execute Customer Due Diligence (CDD). CDD is a vital part of Anti-Money Laundering and Terrorism Financing requirements. It enables the firm to know who its customers are and give a chance to decide whether accept them according to companies' risk appetite.
- Should develop and implement an in-house training program.
- Should be able to evaluate the money laundering risk, identify problems in compliance processes, and analyze them.
- Should ensure that the Company complies with AML regulations. Otherwise, a firm's Compliance Officer may be subject to higher fines or worse sanctions.
- Enforce the implementation of KYC and KYB procedures.
- Reporting to authorities outside of the Company like FCA regularly and to senior management annually.
- Determining the risk level of customers when opening a new customer account.
- Implementing the Company's anti-money laundering compliance policies.
- Analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- Taking protective measures against financial crimes to the Company.
- Detecting and reporting unusual transactions.
- Review all internally reported unusual transactions for their completeness and accuracy with other sources;
- Keep records of internally and externally reported unusual transactions;
- Execute closer investigation of Unusual transactions if necessary,
- Prepare the external report of unusual transactions;

- Make necessary changes to the AML program;
- Remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and •
- Prepare periodic information on the Company's efforts against money laundering and financing of terrorism and proliferation,

In the absence of an express prohibition in the legislature, part of the Compliance Officer's powers may be transferred to another responsible person in the Company to other third parties with appropriate skills.

What are the Responsibilities of MLRO?

- The MLRO shall prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU.

9.1.External reporting procedures

After considering the internal report and all the necessary documentation, when MLRO determines that there is:

(a) knowledge;

(b) suspicion; or

(c) reasonable grounds to suspect that:

- a transaction may be related to ML/TF (regardless of the amount involved); or
- a person may have been, is or may be connected with ML/TF; or
- ML/TF has been, is being or may be committed or attempted;

(b) Transaction amounts surpassing the respective thresholds as indicated per the objective indicators
The following transactions or intended transactions are deemed unusual:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- Transactions in the amount of XCG 5000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:
 - A cashless transaction in the amount of XCG 5000 or more.
 - A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the player.
 - Accepting or releasing a deposit in the amount of XCG 5000 or more at the request of the player;
 - Sale to a player of chips in the amount of XCG 5000 or more. "Chips" include

but is not limited to tokens and credits.

- A cash out in the amount of XCG 5000 or more;

A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of XCG 5000 .

- Presumed money laundering transactions or terrorist financing: Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

The Company is registered with the FIU and has the access to goAML reporting portal.

The MLRO shall file a STR to FIU Curaçao and determines if reporting should also be done to other FIU in the country of an Outsourcing Provider².

The MLRO will not disclose the name of the employee who made the internal report to the FIU, and in completing this report MLRO must provide as much detail as possible together with the relevant identification and other supporting documentation.

The decision to file or not to file an unusual transaction report will always be at the discretion of the MLRO, and MLRO will not be subject to the direction or approval of other parties within the organization, provided that in reaching the decision on whether to file a report, MLRO may seek assistance from other employees of the Company or external advisors.

The MLRO shall prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Company shall report to the FIU the details of the transactions by means of the goAML reporting portal. The reports and the submission of the thereto related information (all supporting documents) shall be done in English.

All unusual individual transactions or series of transactions, as mentioned in the Regulation Indicators Unusual Transactions, shall be reported internally, without any delay. Also supporting documents must be submitted as part of the reporting

Prohibition of Disclosure

The Company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU.

It is forbidden to disclose information to the customer nor to third parties.

Drastic action should only be taken when there is no other way out, since any unjustified action may alert the player. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

While external disclosure is prohibited, internal communication within the reporting entity may be permitted as necessary to ensure compliance with AML/CTF/CPF obligations.

Any disclosure that could prejudice an ongoing or potential investigation by the FIU is illegal.

16. Technological Developments Risk Assessment

The Company has implemented Controls to Prevent the Misuse of Technological Developments for the purposes of Money Laundering and Terrorist Financing. It helps identify and assess the money laundering

or terrorist financing risks that may arise whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

Controls to Prevent the Misuse of Technological Developments for Money Laundering and Terrorist Financing include:

16.1. Business Partner Verification and Monitoring

Enhanced Know Your Business (KYB) Procedures require verification for all new business partners using registers of partners jurisdiction registration and verification through the list of companies check- resources that also include social media.

16.2 Continuous Monitoring.

Continuously monitor business partners behavior using advanced analytics and machine learning algorithms to detect unusual patterns indicative of ML/TF. Regularly update and refine monitoring algorithms to stay ahead of emerging threats and typologies.

16.3. Secure Platform Development.

Used to ensure that all new technological developments, including software and systems, are designed with security and AML/CFT/CPF compliance in mind from the outset. Conduct thorough security assessments and penetration testing on new technologies before deployment.

16.4. Access Controls and Data Security.

Implementing of strict access controls to ensure that only authorized personnel have access to sensitive systems and data. Use encryption and secure communication protocols to protect customer data and transaction information.

16.5. Product and Service Controls

16.5.1. New Product Risk Assessment. Conduction of a detailed risk assessment for ML/TF whenever a new product or service is developed, including digital wallets, cryptocurrencies, and peer-to-peer transactions. Implement additional controls and monitoring for higher-risk products and services.

16.5.2 Ongoing Product Review. Regularly review and update of risk assessments and controls for existing products and services to account for new threats and vulnerabilities. Involve cross-functional teams, including compliance, legal, and IT, in the review process.

16.6. Staff Training and Awareness

16.6.1 Training Programs. Provision of ongoing training for employees on the latest ML/TF/PF risks, typologies, and regulatory requirements. Include specific training on the risks associated with new technologies and how to identify and report unusual activities concerning business partners.

17. Awareness and Training

The MLRO shall adopt the appropriate and proportionate measures to:

- 1) ensure that the relevant employees are aware of relevant AML/CTF/CPF legislation and data protection requirements as well as of the Company's policy and procedures

2) provide training in relation to AML/CTF/CPF.

The training shall be provided to all employees, including consultants and temporary hired and outsourced staff, involved in the relevant activity and business of the Company.

The training shall be relevant to the respective employees' specific responsibilities and function within the Company. Through the training the Company shall ensure that the relevant employees are aware of:

1. CDD measures
2. Record keeping procedures
3. Internal and external reporting procedures
4. Customer Acceptant Policy
5. CRA policy
6. Relevant local and international legislation related to AML/CTF/CPF matters

The Company provide separate trainings for employees of different roles:

a) New employees

New employees who will handle customers or their transactions, irrespective of their level of seniority, receive trainings on:

- the nature and process of money laundering and terrorist financing
- the need to report any unusual transactions to the appropriate designated officer.
- awareness of the existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements.
- money laundering methods and trends in the gambling sector.
- customer due diligence
- objective and subjective indicators for reporting unusual transactions

b) Slot department personnel

Slot department personnel receive trainings on

- a general issues concerning the importance of AML and some basics.
- how money launderers might use gambling companies to launder money the need to verify the identity of the player
- basic issues on customer due diligence process

c) Audit staff

Audit staff charged with overseeing, monitoring and testing money laundering controls. Audit staff receive trainings on:

- changes in regulation,
- changes in money laundering methods and enforcement, and their impact on the organization
- basic process of money laundering and its threats to the Company

d) AML Compliance staff

AML Compliance staff is fully responsible for AML stability in the Company.

They shall need specialized training to be able to stay on top of new trends or changes that impact the organization and the way it manages risk.

AML Compliance staff shall attend conferences or AML-specific presentations to go into greater detail.

Also, AML Compliance staff shall take all new courses on AML

e) Supervisors and Managers

A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.

f) Senior management and board of directors

Money laundering issues and dangers are regularly and thoroughly communicated to the board. This to keep board members aware of the reputational risk that money laundering poses to the institution.

The Company refresh training every three months to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends. In case, there are some crucial changes in AML unscheduled trainings are provided urgently for the respective staff members.

- **Methods of Delivery:**

- Instructor-led training (in-person or virtual)
- Scenario-based workshops and table-top exercises
- Interactive e-learning modules with assessments
- Customized role-specific learning paths

All training records are retained for a minimum of **five (5) years** or longer if required by applicable regulations or during ongoing investigations.

Oversight, Review, and Continuous Improvement

- The **Compliance Officer** is responsible for developing, updating, and implementing the training program and reporting its effectiveness to senior management and, where required, the Board.
- The training curriculum is reviewed **at least annually** to incorporate:
 - Changes in applicable laws and regulations
 - Updates to the Company's business model, products, or geographic exposure
 - Findings from internal audits, FIU feedback, or regulatory reviews
- Metrics such as training completion rates, incident reports, and employee assessments are used to refine and strengthen the program continuously.

The Company shall keep a record of training in which are included the following information:

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

The Compliance Officer shall be responsible for designing and maintaining the Company's AML training materials. All the relevant employees shall undergo AML training upon commencement of their work and then have regular refreshers at least once a year.

The Company should devise and implement a clear and well-articulated policy and procedure for ensuring that relevant employees are aware of their legal obligations in respect of the prevention of money laundering, terrorist financing and proliferation financing, and for providing them with regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering, terrorist financing or proliferation financing. The Company should also monitor the effectiveness of such training, to ensure that all employees are trained in an appropriate and timely manner, and that the training is fit for purpose.

Screening of new employees:

Screening new employees is a critical process to ensure compliance with legal and regulatory requirements, maintain a high standard of integrity, and protect the Company's reputation. Here are the key aspects to consider when screening new employees:

1. Legal and Regulatory Compliance

The Company must adhere to various local and international regulations, such as anti-money laundering (AML) laws, responsible gambling guidelines, and licensing conditions. The screening process should ensure that all new hires comply with these regulations.

2. Background Checks

Conduct thorough background checks to verify the identity, criminal history, financial background, and employment history of potential employees. This may include:

- **Criminal Record Check:** Ensuring that the candidate does not have a history of criminal activity, especially related to fraud, theft, or any form of gambling-related offenses.
- **Credit Check:** Assessing the financial stability of the candidate, particularly important for roles involving financial transactions or handling of funds.
- **Employment Verification:** Confirming previous employment history to verify the experience and integrity of the candidate.
- **Education Verification:** Ensuring that the educational qualifications claimed by the candidate are legitimate.

3. Drug and Alcohol Testing

Drug and alcohol testing is a part of the pre-employment screening process to ensure that candidates are not using substances that could impair their judgment or performance.

4. References and Recommendations

The Company collect references from previous employers to gather insights into the candidate's work ethic, reliability, and integrity. This can help in assessing the suitability of the candidate for roles within the Company.

5. Skills and Competency Testing

Evaluation of the specific skills and competencies required for the role. This can include:

- **Technical Skills:** For IT or technical positions, to ensure that the candidate has the necessary technical expertise.
- **Customer Service Skills:** For roles involving direct interaction with players, assessing the candidate's customer service capabilities.
- **Analytical Skills:** Important for roles that involve handling bets, payouts, and financial transactions.

6. Compliance with Responsible Gambling Policies

The Company shall ensure that candidates understand and are committed to promoting responsible gambling practices. This includes awareness of problem gambling signs and the ability to adhere to the Company's policies on responsible gambling.

7. Training and Induction

Once hired, new employees should undergo comprehensive training to understand:

- **Company Policies:** Including AML policies, responsible gambling practices, and customer service standards.
- **Legal Obligations:** Awareness of the legal and regulatory requirements specific to the gambling industry.
- **Operational Procedures:** Detailed training on the Company's operational procedures, security protocols, and ethical standards.

8. Ongoing Monitoring and Evaluation

Even after the initial screening, it is crucial to continually monitor and evaluate employees to ensure ongoing compliance and integrity. This can include:

- **Regular Background Checks:** Periodic re-screening to catch any issues that may arise after hiring.
- **Performance Reviews:** Regular assessments to ensure employees meet performance and ethical standards.

17. Audit

The Company shall provide an independent audit function to test the AML program

The AML compliance program shall be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit of the Company is independent, thus performed by people not involved with the organization's AML compliance staff.

These tests shall include:

- An evaluation of the Company's anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;
- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements;
- An assessment of the adequacy of the record retention system.

The audit team should also consider whether the board was responsive to earlier audit findings.

The scope of the testing and the testing results must be documented, with any deficiencies reported to senior management and/or the Board of Supervisory Directors, and to the designated officers with a request to take prompt corrective actions by a certain deadline.

18. Cooperation with Authorities

The Company commits to fully cooperate with law enforcement and regulatory authorities by providing requested information within five (5) business days, unless otherwise specified by the requesting authority.

The Compliance Officer shall act as the primary liaison for all communications and requests from such authorities.

19. Additional Measures

The Company proactively evaluates technological development risks, which may arise from outdated systems, cyber threats, software errors, hardware malfunctions, or issues affecting data integrity. These risks can directly impact business performance and strategic goals. A comprehensive approach to managing these risks includes identifying, assessing, prioritizing, and mitigating potential threats.

The Company maintains internal controls and procedures to prevent the misuse of technological advancements for money laundering or terrorist financing purposes. A risk assessment must be conducted when:

- A new product is introduced;
- A new business practice is adopted;
- A new delivery channel is implemented;
- New or emerging technologies are applied to new or existing products or services.

Risk assessments must be conducted prior to the implementation of any new product, business practice, delivery mechanism, or technology. These assessments must be documented and any identified risks must be mitigated through appropriate measures.

The Company shall review and update its risk assessments annually, or sooner if significant changes occur, such as the launch of new products, adoption of new payment methods, or updates to regulatory requirements.

If the Company cannot fulfill the required CDD obligations at the point a transaction reaches the relevant

threshold, it may:

- Place all customer funds into a restricted account with no withdrawal capability;
- Allow further deposits into the account, provided they remain locked;
- Permit wagering from the account, but retain any winnings until CDD is completed;
- Unlock the account and resume normal operations once CDD is finalized;
- Terminate the relationship if CDD cannot be completed;
- Return all customer funds, including deposits and winnings, up to the point of reaching the threshold;

Refunds should be made to the original source account and only after appropriate risk assessment. If there is suspicion of criminal proceeds, a report must be submitted to the FIU, or consent must be sought prior to returning any funds.

The Company will continue monitoring such accounts and report unusual activity using relevant fraud detection platforms and authorities.

In accordance with AML regulations, the Company may suspend, block, or close customer accounts and withhold funds. It reserves the right to employ additional verification procedures as needed to ensure full compliance.

Automated Transaction Monitoring: The Company utilizes automated systems to monitor transactions. Transactions exceeding predefined thresholds (e.g., XCG 10,000 or exhibiting unusual patterns) will be flagged for manual review by the Compliance Officer.

20. Customer Notifications

The Company may notify Customers that it is collecting identity verification information in compliance with applicable regulations.

The Company may issue additional notifications to Customers, including but not limited to account termination, account suspension, or warnings.

Notices will be delivered using one or more of the following channels: email, phone call, internal account message, or postal mail.

21. Applicable rules and legislation

Incorporated and having its statutory seat in Curacao the Company is bound by the local legislation with regards to Anti-Money Laundering, Countering Financing of Terrorism and Proliferation of weapons of mass destruction. The local authority in charge with the supervision on AML-CFT-CFP matters for the gaming sector is the Curacao Gaming Control Board.

The following legislation is applicable to the Company and needs to be taken into consideration within this policy and procedures:

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions

- (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
 - National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
 - National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
 - Sanctions National Ordinance (N.G. 2014, no. 55);
 - National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
 - National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
 - National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);
 - Kingdom Sanction Act (N.G. 2016, no. 54);
 - National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
 - National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
 - National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
 - National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
 - National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
 - Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update May 2024.

The Company checks for amendments to all Decrees and Regulations on a regular basis and updates the policies and procedures accordingly to meet any such changes. Besides these regulatory authorities, the Company also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering ('FATF'), the Caribbean Financial Action Taskforce (CFATF) and the Guidelines and instructions of the European Commission.

2.3. This AML-CFT-CPF POLICY AND PROCEDURES applies to all sites and platforms on which the Company operates.

22. Policy Updates and Sanctions Monitoring

The Company will routinely monitor updates to sanctions laws and regulations and revise its AML/CFT/CPF policies and procedures accordingly. These updates may involve lists of suspected terrorists, terrorist organizations, or sanctioned individuals/entities, that the Company checks regularly.

23. Contact Information

For questions or further information regarding this policy, please contact:

 Email: support@zaza.group

 Address: 6248 Kaya Richard J. Beaujon Z/N Landhuis Joonchi II, Curacao.

24. Policy Revision History

June 17, 2025	Policy update (Annual update)
December 01, 2024	Policy update (legal changes)
June 12, 2024	Policy update (legal changes)
May 28, 2024	Policy update (Annual update)
December 12, 2023	Policy update (legal changes)
May 20, 2023	Policy update (Annual update)
May 24, 2022	Initial Policy

APPENDIX 1

LIST OF HIGH-, MEDIUM-, LOW-RISK JURISDICTIONS

High-risk countries include:

1. Afghanistan
2. Algeria
3. Angola
4. Antigua and Barbuda
5. Barbados
6. Bahamas
7. Belarus
8. Bermuda
9. Burkina Faso
10. Burma
11. Bulgaria
12. Bolivia
13. Cameroon
14. Central African Republic Sanctions
15. China
16. Cuba
17. Côte d'Ivoire
18. Democratic People's Republic of Korea.
19. Democratic Republic of the Congo
20. Ethiopia
21. Gibraltar
22. Guatemala
23. Republic of Guinea
24. Haiti
25. Hong Kong
26. Iran
27. Iraq
28. Jamaica
29. Kenya
30. Lao People's Democratic Republic
31. Lebanon
32. Libya
33. Mali
34. Mozambique
35. Monaco
36. Myanmar
37. Namibia
38. Nepal
39. Nicaragua
40. Nigeria
41. Panama
42. Philippines
43. Russia
44. Sint Maarten Kingdom of the Netherlands
45. Senegal
46. Somalia
47. South Africa
48. South Sudan

Syria

49. Tanzania
50. Trinidad and Tobago
51. Uganda
52. United Arab Emirates
53. Vanuatu
54. Venezuela
55. Vietnam
56. Virgin Islands (UK)
57. Yemen

Medium-risk countries include:

1. Albania
2. Bahrain
3. Bhutan
4. Botswana
5. Brunei Darussalam
6. Cape Verde
7. Chile
8. Cook Islands
9. Costa Rica
10. Cyprus
11. Dominican Republic
12. Fiji
13. Georgia
14. Ghana
15. Greece
16. Hungary
17. Italy
18. Kiribati
19. Kuwait
20. Latvia
21. Malaysia
22. Malta
23. Marschall Islands
24. Martinique
25. Mauritius
26. Montenegro
27. Nauru
28. Niue
29. North Macedonia
30. Poland
31. Portugal
32. Puerto Rico
33. Romania
34. Rwanda
35. Seychelles
36. Slovak Republic
37. Slovenia
38. Spain
39. Tonga
40. Tuvalu

Low-risk countries include:

1. Anguilla

2. Aruba, Kingdom of the Netherlands
3. Cayman Islands
4. Croatia
5. Denmark
6. Dominica
7. Finland
8. Grenada
9. Guyana
10. Mali
11. Montserrat
12. New Zealand
13. Norway
14. Philippines
15. Saint Kitts and Nevis
16. Saint Lucia
17. Saint Vincent & the Grenadines
18. Senegal
19. Singapore
20. Suriname
21. Sweden
22. Tanzania
23. The Bahamas
24. Trinidad and Tobago
25. Turks and Caicos Islands