

Company: Bluewave Interactive NV

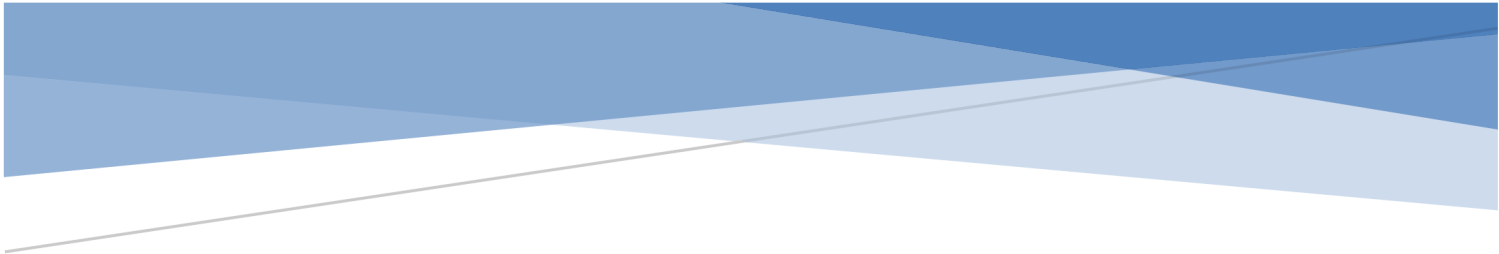
DOCUMENTS INCLUDED

PART I

Business Risk Assessment v1.0 2026

PART II

AML/CFT/CPF Policy v3.0 2026



BUSINESS RISK ASSESSMENT

Bluewave Interactive N.V

Docum ent	Vers ion	Descripti on of Changes	Prepar ed By:	Reviewed By:	Review Date	Approv ed By	Approv al Date	Next Review Date
Busines s Risk Assess ment	1.0	Initial Assessm ent and approval	Compli ance Officer	Chief Legal and Complianc e Officer	20 th July 2026	Board of Directo rs	21 st July 2026	July 2027

CONTENTS

1.	Introduction	3
1.1	Purpose and Scope	3
1.2	Nature of Business.....	3
2.	Definition of Terms	4
3.	Regulatory Framework	5
4.	Governance and Responsibilities	6
4.1	Board of Directors	6
4.2	Senior Management	6
4.3	Compliance Function	6
4.4	MLRO	7
5.	Overall Business Risk Assessment Outcome	7
6.	Risk Appetite	8
7.	Risk Identification Framework	9
8.	Risk Identification	9
8.1	Customer Risk.....	9
8.2	Geographical Risk	11
8.3	Product, Services and Transaction Risk	14
8.4	Delivery Channel Risk	16
9.	Residual Risk Summary	17
10.	Risk Assessment Methodology.....	18
10.1	Table 1- Likelihood Scale	18
10.2	Table 2- Impact Scale.....	19
10.3	Table 3- Inherent Risk.....	19
10.4	Table 4- Effectiveness	20
10.5	Table 5- Residual Risk	20
11.	Review and Update	21
	Annex A. Residual Risk Table	22

1. INTRODUCTION

1.1 PURPOSE AND SCOPE

The purpose of this Business Risk Assessment ("BRA") is to identify, assess, understand, mitigate, and document the risks of money laundering ("ML"), terrorist financing ("TF"), proliferation financing ("PF"), sanctions exposure and associated regulatory, financial and reputational risks to which Corporate Compliance Limited ("the Company") is exposed, taking into account its specific business model, projected client profile, service offering and geographical exposure.

This BRA is designed to:

- support the effective application of a documented and evidence-based risk-based approach ("RBA");
- ensure proportionality of AML/CFT controls;
- provide documented rationale for the Company's risk appetite and control framework;
- serve as the foundation for customer risk assessments ("CRA"), policies and procedures and ongoing monitoring activities;
- demonstrate alignment with the Malta National Risk Assessment, sectoral risk assessments applicable to Company Service Providers, and relevant guidance issued by the FIAU and other competent authorities.

The BRA reflects the nature, scale, complexity and geographic reach of the Company's activities and is aligned with the requirements of the 'Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction as well as sector-specific requirements under the Curacao Gaming Authority

This BRA applies to:

- all business activities, services, and operations of the Company;
- all clients, including prospective, existing and former;
- all jurisdictions of operation, incorporation, residence or source of funds exposure;
- all delivery channels including face-to-face and non-face relationships;
- all employees, officers, directors, the MLRO, Compliance Function and Senior Management.

The BRA applies on a consolidated and entity-wide basis and must be read in conjunction with the Company's AML/CFT Policy, CDD Procedures, and related internal controls, which operationalise the risk findings contained herein.

1.2 NATURE OF BUSINESS

Bluewave Interactive N.V operates as a Business-to-Consumer ("B2C") online gambling operator, providing remote gaming services to individual customers through an internet-based platform. Customers are able to register accounts, deposit funds, participate in gambling activities, and withdraw winnings using approved payment methods.

The Company's business model is characterised by non-face-to-face customer relationships, cross-border customer acquisition, digital payment processing, and the rapid movement of funds through customer accounts. As a result, the Company is exposed to inherent money laundering, terrorist financing, proliferation financing, fraud, sanctions, and other financial crime risks.

The Company offers gambling products through a controlled online environment and maintains systems and controls designed to identify, assess, monitor, and mitigate financial crime risks associated with its operations.

Key characteristics of the Company's business include:

- Remote onboarding and verification of customers through electronic and documentary verification processes;
- Acceptance of customers from approved jurisdictions in accordance with the Company's licensing conditions and risk appetite;
- Processing of deposits and withdrawals through regulated payment service providers and approved payment methods;
- Ongoing monitoring of customer transactions, gambling activity, and behavioural patterns;
- Risk-based customer due diligence, enhanced due diligence, and sanctions screening procedures;
- Automated and manual transaction monitoring controls designed to identify unusual or suspicious activity; and
- Internal reporting and escalation procedures for unusual transactions, suspicious activity, sanctions concerns, and other AML/CFT-related matters.

The Company does not provide banking services, investment services, money remittance services, foreign exchange services, or other financial services outside the scope of its licensed gambling activities.

2. DEFINITION OF TERMS

“AML/CFT” means anti-money laundering and counter-funding of terrorism.

“Beneficial Owner” or “BO” means the natural person(s) who ultimately owns or controls a customer and/or the natural person(s) on whose behalf a transaction or activity is conducted, in accordance with applicable AML/CFT legislation.

“Board” or “Board of Directors” means the Board of Directors of the Company.

“BRA” means the Company's Business Risk Assessment relating to money laundering, terrorist financing, proliferation financing, sanctions, and related AML/CFT risks.

“CDD” means Customer Due Diligence measures carried out in accordance with applicable AML/CFT obligations.

“Company” means Corporate Compliance Limited.

“Compliance Function” means the compliance function responsible for monitoring adherence to applicable legal, regulatory, and internal compliance obligations.

“CRA” means Customer Risk Assessment.

“Customer” means any legal or natural person seeking to establish or maintaining a business relationship with the Company, or carrying out an occasional transaction with the Company.

“EDD” means Enhanced Due Diligence.

“EU” means the European Union.

“FATF” means the Financial Action Task Force.

“FIU” means the Financial Intelligence Unit of Curacao.

“ML” means money laundering.

“ML/FT/PF” means money laundering, terrorist financing, and proliferation financing collectively.

“MLRO” means the Money Laundering Reporting Officer appointed by the Company in accordance with applicable AML/CFT requirements.

“PEP” means Politically Exposed Person and includes family members and known close associates where applicable.

“Personnel” means all individuals engaged by the Company, including directors, officers, employees, secondees, consultants, contractors, temporary staff, the MLRO, members of the Compliance Function, and any other persons acting on behalf of the Company.

“PF” means proliferation financing.

“RBA” means risk-based approach.

“Sanctions” means restrictive measures, sanctions regimes, or financial sanctions imposed by the United Nations, European Union, Curacao, or any other applicable competent authority.

“SDD” means Simplified Due Diligence.

“Senior Management” means the persons responsible for the day-to-day management and operation of the Company.

“STR” or “SAR” means a Suspicious Transaction Report or Suspicious Activity Report submitted internally or externally in accordance with applicable AML/CFT obligations.

“TF” means terrorist financing.

“UBO” means Ultimate Beneficial Owner.

“Non-Reputable Jurisdiction” means a jurisdiction identified as having significant deficiencies in its AML/CFT framework, inadequate regulatory oversight, elevated corruption or organised crime exposure, or otherwise presenting heightened financial crime risk, taking into account FATF, EU, FIU, and other relevant international or national sources.

3. REGULATORY FRAMEWORK

This BRA is established in accordance with the applicable legal, regulatory, and supervisory framework governing the prevention of money laundering, terrorist financing, proliferation financing, sanctions compliance, and the provision of gaming services in Curacao, as amended from time to time.

In particular, this BRA has been developed having regard to, *inter alia*:

- National Ordinance on Identification when rendering Services (“NOIS”)
- National Ordinance on the Reporting Unusual Transactions (“NORUT”)
- Sanctions National Ordinance
- Kingdom Sanction Act
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

This BRA shall be interpreted and applied in a manner consistent with the Company’s broader governance, risk management, and AML/CFT framework, including the Company’s Business Risk Assessment (“BRA”), AML/CFT Policy, Customer Due Diligence (“CDD”) Procedures, and other related internal policies, procedures, and controls adopted by the Company from time to time.

4. GOVERNANCE AND RESPONSIBILITIES

4.1 BOARD OF DIRECTORS

The Board of Directors is responsible for:

- approving the Business Risk Assessment
- defining and overseeing the Company’s risk appetite and ensuring it remains aligned with the Company’s business model and risk exposure;
- ensuring adequate resources, staffing and systems are allocated for AML/CFT compliance;
- reviewing the BRA at least annually and whenever material changes occur;
- exercising effective oversight over the MLRO and Compliance Function.

4.2 SENIOR MANAGEMENT

The Senior Management is responsible for:

- implementing controls at an operational level;
- ensuring day-to-day effectiveness of AML/CFT measures;
- ensuring that customer onboarding, monitoring and risk assessment processes reflect the risk findings set out in the BRA;
- ensuring staff are adequately trained and competent to implement AML/CFT controls.

4.3 COMPLIANCE FUNCTION

The Compliance Function is responsible for:

- monitoring adherence to this BRA;
- performing periodic testing and reviews;
- tracking regulatory and legislative developments;
- documenting findings from compliance reviews and escalating deficiencies to Senior management and the Board where necessary.

4.4 MLRO

The Money Laundering Reporting Officer ("MLRO") is responsible for:

- maintaining and updating the BRA;
- ensuring alignment between the BRA, CRA and AML/CFT framework;
- reporting material risks and deficiencies to the Board;
- ensuring the effective implementation of the risk-based approach across onboarding and ongoing monitoring processes;
- maintaining independence in the performance of duties and having direct access to the Board.

5. OVERALL BUSINESS RISK ASSESSMENT OUTCOME

Bluewave Interactive N.V. operates as a Business-to-Consumer ("B2C") online gambling operator offering providing remote gaming services to individual customers through an internet-based platform. The Company recognised that it is inherently exposed to elevated ML/FT/PF risk due to:

- Non-face-to-face customer relationships;
- Cross-border customer activity;
- Digital onboarding processes;
- The movement of funds through customer accounts;
- The potential misuse of gambling services for money laundering purposes

These structural sector characteristics create inherent vulnerability which cannot be fully eliminated through controls.

Accordingly, the Company assesses its overall inherent ML/TF/PF risk exposure as **High**, having regard to the nature of its business activities, customer base, geographical reach, transaction flows, and the recognised risk profile of the online gambling sector.

In determining its residual risk exposure, the Company has considered the effectiveness of its AML/CFT control framework, including:

- A documented AML/CFT governance framework supported by senior management oversight and an independent MLRO function;
- Risk-based customer onboarding, customer due diligence, and customer risk assessment procedures;
- Customer identity verification controls and ongoing customer due diligence measures;
- Sanctions, Politically Exposed Person ("PEP"), and adverse media screening processes;
- Enhanced Due Diligence measures for higher-risk customers and relationships;
- Source of Funds and Source of Wealth verification procedures where required;
- Automated and manual transaction monitoring controls designed to identify unusual and suspicious activity;
- Ongoing monitoring of customer transactions, gambling activity, and behavioural patterns;
- Defined trigger events and escalation procedures for higher-risk activity;

- Internal reporting, investigation, and regulatory reporting procedures for unusual transactions and suspicious activity;
 - Customer acceptance, restriction, and termination procedures aligned with the Company's risk appetite;
 - Employee AML/CFT training and awareness programmes; and
- Periodic review and testing of AML/CFT controls and risk management processes.

Following assessment of the design, implementation, and effectiveness of the above controls, the Company has determined its overall residual ML/TF/PF risk exposure to be **Medium**.

This assessment reflects the Company's view that while the online gambling sector remains inherently exposed to elevated financial crime risks, the Company's AML/CFT framework is appropriately designed and implemented to identify, manage, mitigate, and monitor those risks to a level consistent with the Company's risk appetite and regulatory obligations.

6. RISK APPETITE

The Company defines its risk appetite as the level and type of money laundering and terrorist financing ("ML/FT") risk it is willing to accept during its business activities, taking into account its regulatory obligations, business model, and risk exposure

The Company adopts a conservative risk appetite and shall only establish or maintain business relationships where the ML/FT risks can be effectively identified, assessed, managed, and mitigated through appropriate controls

As a general principle:

Customers classified as Low, Medium, or High Risk may be accepted, subject to the application of proportionate Customer Due Diligence ("CDD") and ongoing monitoring measures

The Company shall not enter into or continue business relationships where:

- The identity of the customer or beneficial owner cannot be adequately verified
- The customer is subject to applicable sanctions or restrictive measures
- The customer refuses to provide required information or documentation; or
- The ML/FT risk cannot be effectively mitigated

The Company's risk appetite shall be reviewed periodically and updated where necessary to reflect changes in the Business Risk Assessment ("BRA"), regulatory expectations, or the Company's business activities

Risk Level	Definition	Company Risk Appetite	Required Action
Low	Limited likelihood and impact	Acceptable within routine control environment	Routine and periodic monitoring.
Medium	Moderate likelihood and impact	Acceptable with monitoring	Enhanced oversight and risk-based monitoring measures.
High	High likelihood and impact	Low Tolerance (restricted acceptance)	Enhanced due diligence and Senior Management approval prior to onboarding or continuation of relationship.
Extreme	Severe likelihood and impact	Outside standard risk appetite	Board approval required and documented risk justification; relationships shall not be onboarded or maintained.

High-risk relationships may be accepted on an exceptional and risk-justified basis where:

- Enhanced Due Diligence is applied and documented;
- Senior Management approval is obtained;
- residual risk remains within the risk appetite;
- appropriate ongoing monitoring and risk mitigation measures are implemented.

Extreme risk clients fall outside the Company's standard appetite and requires documented Board approval supported by a clear risk justification, and such relationships will generally not be established or maintained.

7. RISK IDENTIFICATION FRAMEWORK

The Company assesses risk through three core components in accordance with its risk-based approach to ML/FT/PF risk management:

Component	Definition
Threat	The likelihood that the Company's services, products or delivery channels may be misused for money laundering, terrorist financing or proliferation financing purposes.
Vulnerability	Weaknesses in systems, controls, processes, or service design that could be exploited to facilitate ML/FT/PF activity.
Consequence	The potential regulatory, legal, financial, operational or reputational impact arising where ML/FT/PF abuse occurs, including supervisory action or enforcement measures.

8. RISK IDENTIFICATION

8.1 CUSTOMER RISK

The Company is exposed to customer-related ML/TF/PF risks arising from the onboarding and ongoing management of individual customers using its online gambling platform, including: onboarding of legal persons and arrangements;

- non-face-to-face customer onboarding and account registration;
- presence of Politically Exposed Persons (“PEPs”), their family members, and close associates
- Customers subject to sanctions screening alerts or adverse media findings; Customers unwilling or unable to provide requested due diligence information or supporting documentation;
- Difficulties in establishing or verifying source of funds and source of wealth information;
- Customers exhibiting behaviour inconsistent with their known profile, occupation, or financial circumstances;
- High-value customers whose gambling activity exceeds expected behavioural norms;
- Customers providing false, misleading, incomplete, or inconsistent information;
- Customers suspected of acting on behalf of third parties;
- Customers linked to fraud, identity theft, account misuse, or other financial crime concerns; and
- Customers displaying unusual or suspicious behaviour during onboarding or throughout the business relationship.

Threats

The Company identifies the following ML/TF/PF threats arising from its customer base:

- Criminals seeking to use gambling services to launder proceeds of crime;
- Individuals attempting to conceal the origin or ownership of illicit funds;
- PEPs seeking to disguise proceeds derived from corruption or abuse of public office;
- Fraudsters and identity thieves attempting to establish or access customer accounts;
- Third parties seeking to use customer accounts to move or transfer funds;
- Organised criminal groups exploiting online gambling services for money laundering purposes; and
- Customers seeking to circumvent AML/CFT controls through deception, misrepresentation, or concealment.

Vulnerability

The Company assesses the following internal and structural vulnerabilities which may be exploited by high risk customers:

- Reliance on information and documentation provided by customers;
- Difficulties in independently verifying source of funds and source of wealth information;
- Limited visibility over a customer's financial circumstances outside of the gambling relationship;
- Potential use of false, forged, or misleading documentation;
- Reliance on customer declarations regarding occupation, income, and financial position;

- The potential for customers to conceal beneficial ownership or third-party involvement in funding activities; and
- The evolving nature of financial crime typologies involving online gambling services.

Inherent Risk: High

The inherent customer risk is assessed as High due to the Company's exposure to a diverse customer base, the potential for customers to conceal the origin of funds, and the recognised susceptibility of the online gambling sector to financial crime.

Mitigating Controls:

- Customer identification and verification;
- Source of Wealth and Source of Funds assessment;
- PEP screening and EDD procedures;
- sanctions and adverse media screening;
- Senior Management approval for high-risk clients;
- ongoing monitoring and periodic risk reviews;
- refusal policy where ownership transparency is inadequate;
- Escalation procedures where inconsistencies or red flags are identified during onboarding or ongoing monitoring.

Likelihood	Impact	Inherent	Mitigation
High	High	High	Effective

Control effectiveness is assessed as "Effective" on the basis that controls are implemented, documented and subject to oversight; however, inherent sector risk remains elevated and cannot be reduced to Low.

8.2 GEOGRAPHICAL RISK

Geographical risk arises from the jurisdictions connected to the Company's customers, customer activity, source of funds, payment flows, and the locations from which customers access the Company's online gambling platform.

The Company recognises that certain jurisdictions may present elevated ML/TF/PF risks due to deficiencies in AML/CFT frameworks, high levels of corruption, organised crime, sanctions exposure, political instability, terrorism risks, or limited regulatory oversight.

As a cross-border online gambling operator, the Company may be exposed to customers from multiple jurisdictions, each presenting varying levels of AML/CFT risk.

Threat Assessment

The Company identifies the following ML/TF/PF threats associated with geographical exposure:

- Customers residing in jurisdictions with weak AML/CFT frameworks or ineffective regulatory oversight;
- Customers connected to countries identified by the FATF as High-Risk Jurisdictions or Jurisdictions under Increased Monitoring;
- Customers located in jurisdictions subject to international sanctions, embargoes, or restrictive measures;
- Exposure to jurisdictions with elevated levels of corruption, organised crime, tax evasion, or financial crime;
- Customers connected to politically unstable, conflict-affected, or high-terrorism-risk regions;
- Source of funds originating from higher-risk jurisdictions;
- Customers attempting to access gambling services from restricted or prohibited jurisdictions; and
- Customers using technologies designed to conceal their true geographic location.

Vulnerability Assessment

The Company assesses the following vulnerabilities linked to geographical exposure:

- source of wealth or source of funds originating from higher-risk countries
- Remote onboarding of customers located outside the Company's primary markets;
- Reliance on customer-provided residence and nationality information;
- Difficulties in independently verifying source of funds originating from foreign jurisdictions;
- Cross-border movement of funds through customer accounts;
- Customers maintaining connections to multiple jurisdictions;
- Use of VPNs, proxies, or other location-concealment technologies;
- Potential discrepancies between declared residence, payment method location, and IP geolocation data;
- Limited visibility over foreign regulatory, legal, and economic environments; and
- Evolving geopolitical developments that may affect jurisdictional risk levels.

The Company acknowledges that exposure to multiple jurisdictions increases the complexity of customer due diligence and ongoing monitoring activities and may increase the risk of financial crime where transparency and regulatory standards differ significantly.

Inherent Risk: **Medium**

The inherent geographical risk is assessed as **Medium** due to the cross-border nature of the Company's online gambling activities and the potential exposure to customers from jurisdictions with differing AML/CFT standards and risk profiles.

Mitigating Controls

- Customer jurisdiction screening during onboarding and throughout the customer lifecycle;
- Screening against FATF High-Risk Jurisdictions and Jurisdictions under Increased Monitoring
- Screening against applicable sanctions and restricted country lists;
- Application of an internal jurisdiction risk classification matrix;

- Geolocation and IP monitoring controls;
- Enhanced Due Diligence measures for customers connected to higher-risk jurisdictions;
- Ongoing monitoring of customer activity and geographic indicators;
- Escalation procedures for higher-risk jurisdictional exposure;
- Restrictions on customers from prohibited or unacceptable jurisdictions; and
- Periodic review of jurisdictional risk assessments based on regulatory and geopolitical developments.

Inherent Risk: High

The inherent products, services, and transaction risk is assessed as **High** due to the nature of online gambling services, the movement of customer funds through the platform, the speed of transactions, and the recognised susceptibility of gambling products to misuse for money laundering and other financial crime purposes.

Mitigating Controls

The Company mitigates products, services, and transaction risks through:

- Risk-based customer due diligence procedures;
- Customer Risk Assessment ("CRA") processes;
- Transaction monitoring systems and automated alert generation;
- Ongoing monitoring of customer activity and gambling behaviour;
- Source of Funds and Source of Wealth verification procedures;
- Trigger event monitoring and escalation processes;
- Identification and investigation of unusual transactions and activity;
- Enhanced Due Diligence measures for higher-risk customers;
- Verification of payment method ownership where required;
- Internal reporting and regulatory reporting procedures;
- Account restriction, suspension, and termination procedures; and
- Periodic review of transaction monitoring rules and risk indicators.

Likelihood	Impact	Inherent	Mitigation
Medium	High	High	Effective

Control effectiveness is assessed as "Effective" based on the implementation of jurisdiction screening and escalation procedures, although residual exposure remains due to reliance on external information sources.

8.3 PRODUCT, SERVICES AND TRANSACTION RISK

Product, Services and Transaction Risk arises from the inherent characteristics of the services provided by the Company and the extent to which such services may be misused for money laundering or terrorist financing or proliferation financing purposes.

The Company is exposed to ML/TF/PF risks arising from the nature of its online gambling products and services and the associated movement of funds through customer accounts.

The Company offers remote gambling services through an online platform, allowing customers to deposit funds, participate in gambling activities, and withdraw winnings. The Company's products and services involve the receipt, holding, wagering, and withdrawal of customer funds, creating opportunities for misuse by individuals seeking to disguise, transfer, layer, or integrate illicit proceeds.

The Company recognises that certain gambling activities, transaction patterns, and payment behaviours may increase exposure to financial crime risks.

In addition, the Company offers Player-to-Player ("P2P") functionality which enables customers to participate in games involving other players. While the P2P product is designed for legitimate gaming purposes, it presents additional ML/TF/PF risks as customers may attempt to use gameplay interactions to transfer value between accounts, facilitate collusive activity, disguise the movement of funds, or create the appearance of legitimate gambling activity.

Threat Assessment

The Company identifies the following ML/TF/PF threats associated with its products, services, and transaction activity:

- Criminals seeking to use gambling products to launder proceeds of crime;
- Customers attempting to transfer, layer, or disguise the origin of illicit funds through gambling activity;
- Rapid deposits followed by withdrawals with little or no genuine gambling activity;
- Customers attempting to create a legitimate appearance for illicit funds through gambling winnings;
- Structuring of deposits, withdrawals, or other transactions to avoid monitoring controls or reporting thresholds;
- Use of multiple payment methods to obscure the origin or destination of funds;
- Third-party funding arrangements designed to conceal beneficial ownership of funds;
- Abuse of gambling products for purposes other than legitimate recreational gambling;
- Use of gambling accounts as a mechanism to transfer value between parties; and
- Fraudulent activity involving deposits, withdrawals, chargebacks, or payment instrument
- Abuse of Player-to-Player ("P2P") functionality to transfer value between customer accounts under the guise of legitimate gameplay;
- Collusion between players to intentionally transfer funds through gaming activity;
- Chip dumping, soft play, coordinated betting, or other gameplay manipulation techniques designed to facilitate value transfers;
- Use of P2P products to disguise the movement, layering, or integration of illicit funds;

- Multiple customers acting in concert to circumvent transaction monitoring controls; and
- Use of P2P activity to create an artificial appearance of legitimate gambling losses or winnings

Vulnerability Assessment

- The ability for customers to rapidly deposit, wager, and withdraw funds through online accounts;
- Reliance on electronic payment methods and payment service providers;
- The potential use of multiple funding sources and payment instruments;
- Difficulties in determining the ultimate origin of customer funds without additional due diligence;
- The possibility of customers engaging in gambling activity primarily for financial crime purposes rather than entertainment;
- High transaction volumes and velocity associated with online gambling operations;
- Potential abuse of bonuses, promotions, or other incentives;
- The use of multiple customer accounts or linked accounts;
- The ability to conduct transactions remotely without face-to-face interaction; and
- Evolving money laundering typologies involving online gambling products and digital payment channels.
- The inherent difficulty in distinguishing legitimate P2P gameplay from collusive or value-transfer activity;
- Potential misuse of P2P functionality to transfer value between related or connected customers;
- The possibility of coordinated activity involving multiple customer accounts;
- Reliance on transaction monitoring and behavioural analytics to detect collusion, chip dumping, soft play, or other forms of gameplay manipulation;
- Increased complexity in identifying beneficial ownership and control of funds where multiple players are involved in the same gaming activity; and
- The potential for sophisticated customers to structure gameplay activity in a manner that resembles legitimate gambling behaviour while facilitating the movement of funds.

The Company acknowledges that the movement of funds through customer accounts presents an inherent financial crime risk and requires ongoing monitoring and scrutiny to identify unusual or suspicious activity.

Inherent Risk: High

The inherent product, service and transaction risk is assessed as **High** due to the nature of online gambling products, the movement of customer funds through the platform, and the additional risks associated with Player-to-Player ("P2P") functionality, which may be susceptible to collusive behaviour and value transfer schemes.

Likelihood	Impact	Inherent	Mitigation
High	High	High	Effective

Control effectiveness is assessed as “Effective” on the basis that mitigating measures are implemented and subject to governance oversight; however, residual exposure remains due to the nature of CSP services.

8.4 DELIVERY CHANNEL RISK

Delivery Channel Risk arises from the manner in which the Company establishes and maintains its business relationships, particularly where services are provided without physical interaction.

The Company is exposed to ML/TF/PF risks arising from the delivery channels through which customers access its products and services. As a B2C online gambling operator, the Company conducts all customer interactions remotely through its online platform without any face-to-face contact with customers.

The Company's business model relies on digital onboarding, remote customer verification, electronic communications, and online account access, which may create opportunities for criminals to conceal their identity, location, or activities.

The Company recognises that the use of technology and remote delivery channels increases the risk of impersonation, identity fraud, account misuse, and other financial crime threats if not adequately controlled.

Threat Assessment

The Company identifies the following ML/FT/PF threats associated with its delivery channels:

- identity fraud during remote onboarding;
- use of forged or manipulated identification of documentation;
- reduced ability to assess behavioural indicators in non-face-to-face relationships.
- Individuals attempting to access the platform from prohibited or restricted jurisdictions;
- Account takeover attacks through compromised credentials or social engineering;

Vulnerability Assessment

The Company assesses the following vulnerabilities linked to delivery channels

- Absence of face-to-face interaction with customers;
- Reliance on electronic customer identification and verification processes;
- Dependence on customer-provided information during onboarding;
- Potential use of forged, altered, or fraudulently obtained documents;
- Challenges in verifying a customer's true physical location;

Inherent Risk Level: **High**

The inherent risk is assessed as High due to the increased risk of impersonation, document manipulation and reduced verification certainty associated with non-face-to-face onboarding.

Mitigating Controls

- application of risk-based Customer Due Diligence;
- independent verification of identification documentation;
- screening against relevant databases;
- enhanced due diligence for higher risk customers;
- escalation procedures where applicable;
- refusal of onboarding where identification or verification requirements cannot be satisfactorily completed;

Likelihood	Impact	Inherent	Mitigation
High	High	High	Effective

Control effectiveness is assessed as “Effective” on the basis that identification and verification procedures are implemented and subject to oversight; however, residual exposure remains due to inherent limitations of remote onboarding.

9. RESIDUAL RISK SUMMARY

The following sets out the Residual Risk assessment after consideration of the effectiveness of mitigating controls. Residual risk is reassessed at least annually and whenever material changes occur to the Company’s business model, client base, services or external risk environment.

Residual Risk is determined by assessing the level of Inherent Risk in conjunction with the assessed effectiveness of mitigating controls, in accordance with the methodology outlined in Section 10 below.

Residual Risk Table

Residual risk ratings below reflect the Company’s current control framework and are based on a qualitative assessment of control design and implementation, taking into account the Company’s business model and governance structure. Control effectiveness ratings are subject to periodic review and validation through compliance monitoring and oversight.

Risk Category / Identification	Inherent Risk	Control Effectiveness (Design and Implementation)	Residual Risk	Risk Within Appetite Y/N
Customer Risk	High	Effective	Medium	Yes

Geographical Risk	Medium	Effective	Medium	Yes
Product / Service / Transaction Risk	High	Effective	Medium	Yes
Delivery Channel Risk	High	Effective	Medium	Yes

Note:

The consistent “Effective (3)” control rating reflects the Company’s standardised AML/CFT control framework applied across all risk categories. The Company acknowledges that residual exposure remains due to inherent Gaming sector risk and therefore residual risk is not reduced below Medium. Control effectiveness is subject to ongoing monitoring and independent review.

10. RISK ASSESSMENT METHODOLOGY

The Company applies a structured methodology that:

- identifies inherent risk;
- evaluates likelihood and impact;
- assesses control and effectiveness;
- determines residual risk.

The assessment is qualitative in nature and is based on the Company’s business model, expected client profile, service offering, and operating environment.

This methodology supports the Company’s risk based-approach and ensures that risks are assessed in a consistent, objective and proportionate manner, and that risk assessments at customer level (CRA) are aligned with the overarching findings of this BRA.

Risk ratings are subject to periodic review and governance oversight to ensure continued appropriateness and accuracy.

10.1 TABLE 1- LIKELIHOOD SCALE

Likelihood refers to the probability that a specific money laundering, terrorist financing or proliferation financing risk event could occur, taking into account:

- the Company’s business model;
- client profile;
- service characteristics;
- geographical exposure;
- external risk environment.

Likelihood assessments are determined on a forward-looking basis and do not rely solely on historical incident data, given the nature of a newly licensed entity.

Risk Level	Likelihood
Low	Unlikely to occur based on the Company's business model, control environment and exposure; limited vulnerability and rare opportunity for misuse.
Medium	Possible occurrence; exposure exists but is not frequent or widespread, and vulnerabilities are limited or controlled.
High	Likely to occur due to significant exposure, structural vulnerabilities, or elevated risk associated with the Company's services, clients or operating environment.
Extreme	Highly likely to occur due to severe exposure or critical vulnerabilities, presenting a persistent or imminent risk requiring immediate mitigation or avoidance.

10.2 TABLE 2- IMPACT SCALE

Impact scale refers to the potential consequences should the risk materialise, considering regulatory, financial, operational and reputational factors

Impact scoring incorporates consideration of:

- regulatory enforcement action by FIU or CGA;
- administrative penalties;
- suspension or revocation of license authorisation;
- reputational damage;
- civil or contractual liability exposure;
- increased supervisory scrutiny; Potential impact on the Company's ability to obtain or maintain regulatory approvals.

Risk Level	Impact of ML/FT/PF Risk
Low	Limited regulatory concern and minimal financial, operational or reputational impact.
Medium	Regulatory scrutiny possible, with moderate financial, operational or reputational impact.
High	Serious regulatory breach or supervisory finding, significant financial loss, reputational damage or enforcement action.
Extreme	Severe regulatory breach, substantial financial or reputational damage, or supervisory action that may materially impact the Company's authorisation or ability to operate.

10.3 TABLE 3- INHERENT RISK

Inherent risk represents the level of money laundering and terrorist financing and proliferation financing risk to which the Company is exposed before the application of any mitigating controls.

Inherent risk is assessed based on the nature of the Company's services, client profile, geographical exposure and delivery channels, taking into account sector-specific vulnerabilities applicable to Company Service Providers.

The assessment reflects the Company's structural exposure to ML/FT/PF risk and is determined on a qualitative and forward-looking basis.

The inherent risk matrix below provides a structured framework for assessing inherent ML/FT/PF exposure based on the interaction between likelihood and impact. The matrix serves as a guiding tool and does not replace professional judgement. Risk ratings are determined through qualitative assessment of the Company's business model, services, client profile and operating environment and are subject to review by the MLRO and governance oversight.

Likelihood ↓	Impact →			
	Low	Medium	High	Extreme
Low	Low	Low	Medium	High
Medium	Low	Medium	High	High
High	Medium	High	High	Extreme
Extreme	High	High	Extreme	Extreme

10.4 TABLE 4- EFFECTIVENESS

Control effectiveness is assessed based on the design, implementation and operational performance of AML/CFT controls, taking into account governance oversight, compliance monitoring and the Company's control environment. The effectiveness rating reflects the extent to which mitigating measures reduce identified risks in a consistent and proportionate manner.

Level of Mitigation	Description of Effectiveness
Strong	Mitigating measures are fully implemented, fully operational, subject to oversight and consistently effective.
Effective	Risk is managed adequately; controls are implemented and operating effectively, though improvements may be identified through monitoring or review.
Ineffective	Risk is not managed adequately; substantial improvements are required, though controls have limited effect.
Non-existent	Controls are absent or ineffective

10.5 TABLE 5- RESIDUAL RISK

Residual risk reflects the level of risk remaining after consideration of the effectiveness of mitigating controls and is determined using a risk-based and qualitative assessment.

Where mitigating controls are assessed as Strong or Effective:

- medium inherent risk shall not be reduced below Medium;
- high inherent risk may be reduced to Medium but not to Low;
- extreme inherent risk may be reduced to High but not to Medium or Low.

This approach reflects the Company's recognition that inherent sector risk associated with gaming activities that cannot be fully eliminated through controls and therefore residual risk remains proportionate to the underlying exposure. Residual risk ratings are subject to governance oversight and periodic review.

The residual risk matrix provides a structured framework for determining the level of risk remaining after consideration of control effectiveness. The matrix serves as a guiding tool and does not replace professional judgement. Residual risk ratings are determined through qualitative assessment of the effectiveness of mitigating controls, taking into account the Company's business model and inherent sector exposure, and are subject to review by the MLRO and governance oversight.

Likelihood ↓	Impact →			
	Low	Medium	High	Extreme
Low	Low	Low	Medium	Medium
Medium	Low	Medium	Medium	High
High	Medium	Medium	High	High
Extreme	Medium	High	High	Extreme

11. REVIEW AND UPDATE

The Business Risk Assessment will be reviewed at least annually and updated whenever material changes occur to the Company's business model, operations or risk environment.

The review process is coordinated by the MLRO and approved by the Board of Directors.

The BRA must be revised in response to external developments, such as:

- The introduction of new products, services, games, or platform functionality, including Player to-Player ("P2P") products;
- Entry into new markets or acceptance of customers from new jurisdictions;
- Significant changes to customer demographics, customer behaviour, or customer risk profile;
- Material changes to applicable laws, regulations, licensing conditions, or regulatory guidance;
- Findings arising from internal audits, compliance reviews, independent testing, or regulatory inspections;

All updates to this BRA shall be documented and communicated to relevant staff, and any material changes shall be subject to Board approval.

ANNEX A. RESIDUAL RISK TABLE

A. Customer Risk

Risk Driver / Scenario	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
Onboarding of legal persons, non-resident customer	- Formation of legal persons with complex ownership chains - Multi-layered ownership structures - Non-resident UBOs and cross-border ownership - Limited transparency in foreign registries	- Identification and verification of Ultimate Beneficial Owner (UBO) - Verification of ownership structure to natural person level - Independent verification of corporate documentation via official registries - Apostilled or notarised documentation where applicable - Source of Wealth and Source of Funds assessment - Ongoing monitoring and periodic review - Refusal where ownership transparency is inadequate	- Jurisdictional opacity may remain - Deliberate structuring to obscure ownership - Delays in identifying ownership changes - Registry reliability varies by jurisdiction
Presence of Politically Exposed Persons (PEPs)	- Exposure to corruption risk - Potential abuse of corporate structures - Elevated regulatory scrutiny	- PEP screening and identification procedures - Enhanced Due Diligence (EDD) - Senior Management approval - Ongoing monitoring and periodic review	- Corruption exposure risk remains - Heightened regulatory and reputational risk - Risk of misuse of funds cannot be fully eliminated
Misrepresentation of Source of Wealth or Source of Funds	- Reliance on customer-provided information - Complex wealth structures - Cross-border financial arrangements	- Supporting documentation validation - Source of Wealth and Source of Funds assessment - Risk-based escalation procedures	- Documentation may be manipulated - Complex structures may obscure origin of funds - Cross-border verification limitations

Risk Driver / Scenario	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
Player with adverse media or regulatory concerns	- Reputational exposure - Potential regulatory or criminal history - Increased ML/FT/PF risk indicators	- Adverse media screening - Risk-based assessment and escalation - Senior Management approval where required - Ongoing monitoring	- Reputational risk persists - Media sources may not capture all misconduct - Ongoing investigations may not be publicly available

B. Geographical Risk

Inherent Risk Level: Medium

Control Effectiveness: Effective

Residual Risk Level: Medium

Geographical Risk Driver / Scenario	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
Player resident in jurisdictions with weak AML/CFT supervision	- Weak regulatory enforcement - Limited transparency of beneficial ownership - Poor quality or reliability of public records	- Screening against FATF high-risk and increased monitoring lists - Screening against EU high-risk third-country lists - Jurisdiction risk classification matrix - Enhanced Due Diligence (EDD) where required - Escalation to MLRO/Senior Management	- Possibility of undisclosed criminal exposure due to weak local enforcement - Reliance on external registry information may limit full transparency
Exposure to jurisdictions identified as high-risk or under increased monitoring by FATF or EU	- Elevated systemic ML/FT/PF risk - Increased corruption or organised crime indicators - Heightened sanctions or regulatory exposure	- Prohibition of blacklisted jurisdictions - Mandatory EDD for increased monitoring jurisdictions - Senior Management approval - Ongoing enhanced monitoring	- Customers may attempt layered structuring to conceal links to high-risk jurisdictions - Rapid geopolitical changes may affect risk classification
Jurisdictions with high corruption or organised crime levels	- Increased risk of illicit wealth generation - Potential falsified documentation	- Corruption risk assessment (e.g., Transparency International index)	- Risk of falsified or manipulated documentation may not always be detectable

Geographical Risk Driver / Scenario	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
	- Regulatory or enforcement gaps	- Enhanced Source of Wealth verification - Risk-based escalation procedures	- Corruption exposure risk persists despite controls

C. Product, Services and Transaction Risk

Inherent Risk Level: High

Control Effectiveness: Effective

Residual Risk Level: Medium

Service / Risk Driver	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
Online Gaming Products	- Potential misuse of gambling products to disguise illicit funds - High transaction volumes and customer activity - Cross-border customer participation	- Customer Due Diligence (CDD) - Customer Risk Assessment (CRA) - Ongoing transaction and activity monitoring - Source of Funds verification where required	- Gambling products remain vulnerable to misuse for ML/TF/PF purposes despite monitoring controls
Player-to-Player ("P2P") Functionality	- Potential transfer of value between customers - Collusive activity designed to facilitate movement of funds - Difficulty distinguishing legitimate gameplay from value transfers	- P2P transaction monitoring - Player behaviour monitoring - Linked account detection - Enhanced review of unusual activity - Account restrictions and escalation procedures	- Sophisticated collusion or coordinated player activity may not be immediately identifiable
Deposits and Funding Transactions	- Introduction of illicit funds into the platform - Use of multiple funding methods - Third-party funding risks	- No custody or management of client funds - Risk-based monitoring and escalation procedures	- Customers may attempt to conceal the origin or ownership of funds
Withdrawals and Cash-Out Transactions	- Potential extraction of funds appearing to be legitimate gambling proceeds - Movement of funds	- Withdrawal monitoring - Payment method ownership verification - Enhanced Due	- Criminals may attempt to legitimise funds through gambling activity before withdrawal

Service / Risk Driver	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
	to different destinations	Diligence reviews - Unusual transaction reporting procedures	
High-Value and High-Frequency Transactions	- Increased exposure to ML/TF/PF risks - Greater opportunity for layering and movement of funds	- Automated transaction monitoring - Source of Funds and Source of Wealth verification - Enhanced monitoring thresholds - MLRO escalation procedures	- Significant transaction volumes increase financial crime exposure despite enhanced controls
Cross-Border Transactions	- Movement of funds across multiple jurisdictions - Exposure to differing AML/CFT standards and regulatory environments	- Jurisdictional risk assessment - Enhanced Due Diligence for higher-risk jurisdictions - Ongoing monitoring and sanctions screening	- Cross-border activity may increase complexity in identifying and tracing suspicious transactions
Bonus, Promotional and Incentive Features	- Potential abuse of promotions to facilitate movement of funds or artificial gaming activity	- Bonus abuse controls - Transaction and behavioural monitoring - Trigger event reviews	- Customers may attempt to exploit promotional mechanisms in ways that are not immediately detected
Rapid Deposit, Wagering and Withdrawal Activity	- Potential layering or movement of funds through gaming accounts - Activity lacking genuine gambling purpose	- Behavioural monitoring - Deposit-to-withdrawal ratio reviews - Enhanced Due Diligence triggers - Unusual transaction reporting procedures	- Sophisticated money laundering patterns may initially resemble legitimate gambling behaviour

D. Delivery Channel

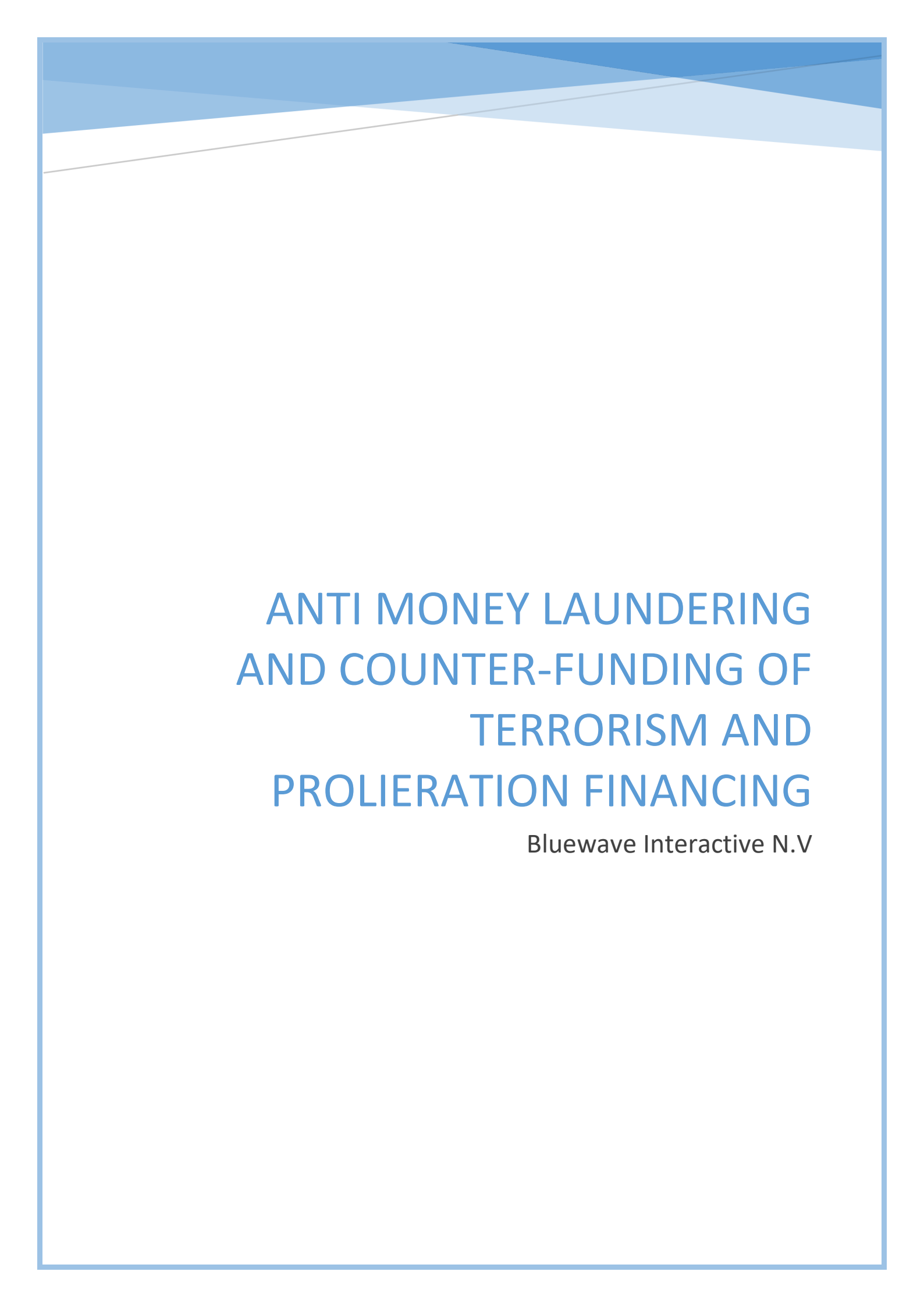
Inherent Risk Level: High

Control Effectiveness: Effective

Residual Risk Level: Medium

Delivery Channel / Risk Driver	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
Remote / non-face-to-face onboarding	- Increased risk of identity fraud or impersonation - Reduced ability to assess behavioural indicators - Reliance on remote verification methods	- Risk-based Customer Due Diligence procedures - Independent identity verification using reliable sources - Additional verification measures for higher-risk customers - Escalation procedures where inconsistencies arise	- High-quality forged or stolen identities may still bypass controls - Remote onboarding inherently reduces verification certainty
Use of forged or manipulated identification documents	- Document falsification risk - Technological manipulation of identity documents - Reliance on customer-provided documentation	- Document authenticity checks - Independent verification of identification data - Risk-based escalation procedures	- Sophisticated forgery or manipulation may not always be detected
Absence of physical presence during customer verification	- Limited direct interaction with client - Reduced ability to validate identity through physical checks	- Verification through independent and reliable data sources - Additional documentation requirements where necessary	- Remote verification methods may not fully eliminate impersonation risk
Reliance on scanned or electronically transmitted documents	- Risk of altered or incomplete documentation - Dependence on electronic transmission integrity	- Requirement for certified copies where appropriate - Independent verification procedures - Supporting documentation review	- Altered or manipulated documents may not always be detectable
VPN, Proxy and Anonymisation Technology Usage	- Ability to mask true location or identity - Circumvention of jurisdictional restrictions	- VPN and proxy detection tools - Device monitoring controls - Enhanced review procedures	- Advanced anonymisation technologies may reduce visibility over customer location and activity
Cross-Border Digital Service Delivery	- Services accessible across multiple jurisdictions - Exposure to varying	- Country restrictions - Geolocation controls - Jurisdictional risk assessments	- Cross-border accessibility increases complexity in monitoring and

Delivery Channel / Risk Driver	Inherent Risk Factors	Key Mitigating Controls	Residual Risk (After Mitigation)
	regulatory and financial crime risks	- Enhanced Due Diligence measures where required	managing ML/TF/PF risks



ANTI MONEY LAUNDERING AND COUNTER-FUNDING OF TERRORISM AND PROLIERATION FINANCING

Bluewave Interactive N.V

Document	Version	Description of Changes	Prepared By:	Reviewed By:	Review Date:	Approved By	Approval Date	Next Review Date
AML/CFT/CPF Policy	3.0	Review and Enhancement – changes made addressing the New AML/CFT Regulations of CGA	Compliance Officer	Chief Legal and Compliance Officer	20 th July 2026	Board of Directors	21 st July 2026	July 2027

CONTENTS

1	Introduction	4
1.1	Purpose.....	4
1.2	Scope	4
2	Definition of Terms	4
3	Regulatory Framework.....	5
4	Governance and Responsibilities	6
4.1	Board of Directors	6
4.2	Senior Management	6
4.3	Compliance Function	6
4.4	MLRO	6
5	Risk Based Approach Framework.....	7
5.1	Business Risk Assessment (BRA)	7
5.2	Customer Risk Assessment (CRA)	7
5.3	Risk Scoring Methodology	7
5.4	Risk Appetite.....	8
6	Customer Risk Assessment	8
6.1	Timing of CRA	8
6.2	Risk Factors	9
	Customer Risk.....	9
	Geographical Risk	10
	Product, Service and Transaction Risk	10
	Delivery Channel Risk	11
7	Technological Risk Assessment	12
8	Customer Onboarding and Due Diligence.....	12
8.1	Customer Acceptance.....	13
8.2	Customer Due Diligence (CDD)	13
8.3	Simplified Due Diligence (SDD)	14
8.4	Enhanced Due Diligence (EDD)	15
9	CDD Measures.....	17
10	Beneficial Ownership	18
10.1	Identification	19
10.2	Verification	19
10.3	Purpose and Intended Nature of Business	20
10.4	Politically Exposed Person (PEPs)	20
10.4.1	Enhanced Due Diligence FOR PEP	20
10.4.2	Senior Management Approval	21
10.5	Sanctions Screening	21
11	Ongoing Monitoring Review	22
11.2	Trigger Events	22

11.3 Review Frequency	23
11.4 Monitoring Measures	24
11.5 Timing of CDD Measures	24
12. Suspicious Activity/Transaction Reporting (SAR/STR)	26
12.1 Internal Reporting	27
12.2 External Reporting	27
12. 3 No Tipping Off.....	27
13. Termination of Business Relationship.....	27
13.1 Account Restriction and Suspension	28
13.2 Termination Decision.....	28
13.3 Return of Customer Funds.....	28
14. Training	29
14.1 Personnel Vetting	29
15. Record Keeping	30
15.1 Records Maintained.....	30
15.2 Retention Period.....	31
16. Independent Audit Function	32
17. Regulatory Supervision and Examination	33
18. Review and Update	33
Annex A- CRA Risk Scoring Methodology.....	35
Annex B- CRA Risk Rating Methodology	38

1 INTRODUCTION

1.1 PURPOSE

This Anti-Money Laundering and Counter-Funding of Terrorism (“AML/CFT”) Policy establishes the framework, principles, controls, and procedures adopted by the Company to prevent its products, services, and business activities from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion, or other financial crime.

This Policy is intended to ensure that the Company maintains effective and proportionate AML/CFT systems and controls in accordance with applicable legal and regulatory obligations, including Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction and other relevant laws, regulations, and regulatory guidance applicable to online gaming company in Curacao

This Policy forms part of the Company’s broader governance, risk management, and compliance framework and shall be applied in conjunction with the Company’s Business Risk Assessment (“BRA”), Customer Due Diligence (“CDD”) Procedures, and related internal policies and procedures

1.2 SCOPE

This Policy applies to all directors, officers, employees, consultants, contractors, and any other persons acting on behalf of the Company.

The Policy applies across all products, services, business relationships, and activities carried out by the Company and shall be complied with throughout the entire lifecycle of the customer relationship, including onboarding, ongoing monitoring, and termination of the relationship

2. DEFINITION OF TERMS

“AML/CFT” means anti-money laundering and counter-funding of terrorism

“Board” or “Board of Directors” means the Board of Directors of the Company.

“BRA” means the Company’s Business Risk Assessment relating to money laundering, terrorist financing, proliferation financing, sanctions, and related AML/CFT risks.

“CDD” means Customer Due Diligence measures carried out in accordance with applicable AML/CFT obligations.

“Company” means Bluewave Interactive N.V

“CRA” means Customer Risk Assessment.

“EDD” means Enhanced Due Diligence.

“FATF” means the Financial Action Task Force.

“FIU” means the Curacao Financial Intelligence Unit

“ML” means money laundering.

“ML/FT/PF” means money laundering, terrorist financing, and proliferation financing collectively.

“MLRO” means the Money Laundering Reporting Officer appointed by the Company in accordance with applicable AML/CFT requirements.

“PEP” means Politically Exposed Person and includes family members and known close associates where applicable.

“Personnel” means all individuals engaged by the Company, including directors, officers, employees, secondees, consultants, contractors, temporary staff, the MLRO, members of the Compliance Function, and any other persons acting on behalf of the Company.

“PF” means proliferation financing.

“RBA” means risk-based approach.

“Sanctions” means restrictive measures, sanctions regimes, or financial sanctions imposed by the United Nations, European Union, Curacao, or any other applicable competent authority.

“Senior Management” means the persons responsible for the day-to-day management and operation of the Company.

“STR” or “SAR” means a Suspicious Transaction Report or Suspicious Activity Report submitted internally or externally in accordance with applicable AML/CFT obligations.

“TF” means terrorist financing.

3. REGULATORY FRAMEWORK

This AML/CFT Policy is established in accordance with the applicable legal, regulatory, and supervisory framework governing the prevention of money laundering, terrorist financing, proliferation financing, sanctions compliance, as amended from time to time

In particular, this Policy has been developed having regard to inter alia:

- National Ordinance on Identification when rendering Services (“NOIS”)
- National Ordinance on the Reporting Unusual Transactions (“NORUT”)
- Sanctions National Ordinance
- Kingdom Sanction Act
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

4. GOVERNANCE AND RESPONSIBILITIES

4.1 BOARD OF DIRECTORS

The Board of Directors are responsible for:

- Approving the Business Risk Assessment
- Defining and overseeing the Company's risk appetite ensuring adequate resources for AML/CFT compliance

The Board shall ensure that the MLRO and Compliance Function are provided with sufficient authority, independence, resources, and access to training effectively discharge their responsibilities

4.2 SENIOR MANAGEMENT

The Senior Management is responsible for:

- Implementing controls at an operational level
- Ensuring day-to-day effectiveness of AML/CFT measures

4.3 COMPLIANCE FUNCTION

The Compliance Function is responsible for:

- Monitoring adherence for this policy and the overall AML/CFT framework
- Performing periodic testing and reviews, including independent testing of the effectiveness of Controls and reporting deficiencies to Senior Management and the Board
- Tracking regulatory and legislative developments

4.4 MLRO

The Money Laundering Reporting Officer is responsible for:

- Receiving, analysing and assessing internal suspicious reports and determining whether to submit STRs/SARs to the FIU
- Ensuring effective internal reporting procedures and acting as the central point of contact with the FIU
- Contributing to the development and periodic review of the BRA in coordination with the Compliance Function and Senior Management and the Board
- Tracking Regulatory and legislative developments

5. RISK BASED APPROACH FRAMEWORK

5.1 BUSINESS RISK ASSESSMENT (BRA)

The Company maintains a Business Risk Assessment (“BRA”) to identify and assess the money laundering, terrorist financing and proliferation financing (ML/FT/PF) risk associated with its business activities, customers, services, delivery channels, and geographical exposure

The BRA forms the basis of the Company’s risk-based approach and supports the application of proportionate AML/CFT controls and measures

The findings of the BRA are taken into account when conducting Customer Risk Assessments (“CRA”) applying Customer Due Diligence”) measures, and determining the level of ongoing monitoring required

5.2 CUSTOMER RISK ASSESSMENT (CRA)

The Customer Risk Assessment (“CRA”) forms a core component of the Company’s risk-based approach and is used to assess and classify the money laundering and terrorist financing (“ML/FT”) risk associated with each customer

The CRA supports the application of proportionate Customer Due Diligence (“CDD”) measures and ongoing monitoring throughout the business relationship

Further detail on the CRA methodology and its application is set out in Annex A on this Policy

5.3 RISK SCORING METHODOLOGY

The Company applies a structured risk scoring methodology as part of its Customer Risk Assessment (“CRA”) framework to support the consistent assessment and classification of customer ML/FT risk

The risk scoring methodology is based on the assessment of customer risk, geographical risk, product and service risk, and delivery channel risk

The operational risk indicators and scoring criteria are set out in Annex A- CRA Risk Scoring Matrix of this Policy,

The outcome of the risk assessment determined the overall customer risk classification and supports the application of proportionate Customer Due Diligence (“CDD”) measures and ongoing monitoring

The methodology shall not replace professional judgement, and the Company may apply a higher risk classification were justified by the specific circumstances of the customer relationship

Any manual override of calculate risk classification shall be documented and appropriately approved.

5.4 RISK APPETITE

The Company defines its risk appetite as the level and type of money laundering and terrorist financing (“ML/FT”) risk it is willing to accept during its business activities, taking into account its regulatory obligations, business model, and risk exposure

The Company adopts a conservative risk appetite and shall only establish or maintain business relationships where the ML/FT risks can be effectively identified, assessed, managed, and mitigated through appropriate controls

As a general principle:

Customers classified as Low, Medium, or High Risk may be accepted, subject to the application of proportionate Customer Due Diligence (“CDD”) and ongoing monitoring measures

The Company shall not enter into or continue business relationships where:

- The identity of the customer or beneficial owner cannot be adequately verified
- The customer is subject to applicable sanctions or restrictive measures
- The customer refuses to provide required information or documentation; or
- The ML/FT risk cannot be effectively mitigated

The Company’s risk appetite shall be reviewed periodically and updated where necessary to reflect changes in the Business Risk Assessment (“BRA”), regulatory expectations, or the Company’s business activities

6. CUSTOMER RISK ASSESSMENT

The Company conducts a Customer Risk Assessment (“CRA”) in respect of each customer to identify, assess, and classify the money laundering and terrorist financing (“ML/FT”) risk associated with the business relationship

The CRA is conducted in accordance with the Company’s risk-based approach and supports the application of proportionate Customer Due Diligence (“CDD”) measures and ongoing monitoring

The CRA shall be performed prior to onboarding and updated accordingly or upon the occurrence of relevant trigger events

The assessment shall consider customer risk, geographical risk, product, service and transaction risk and distribution channel risk

A provisional risk rating shall be assigned during onboarding and subsequently reviewed and updated whenever additional information becomes available, material changes occur, or new risk indicators are identified. The resulting risk classification shall determine the level of due diligence, monitoring, and review required throughout the customer relationship.

6.1 TIMING OF CRA

The Customer Risk Assessment (“CRA”) shall be conducted and maintained on a risk-based throughout the lifecycle of the business relationship

In particular, the CRA shall:

- Be performed prior to the establishment of a business relationship or carrying out of an occasional transaction;
- Be reviewed periodically in accordance with the customer's assigned risk rating, as determined through the risk scoring methodology set out of this Policy
- Be updated without undue delay upon the occurrence of any trigger event that may impact the customer's risk profile, and
- Be appropriately documented and retained in accordance with the Company's record-keeping obligations

The Company shall ensure that the CRA determined using the risk scoring methodology remains accurate, up to date, and reflective of the customer's current risk profile at all times

6.2 RISK FACTORS

The Customer Risk Assessment ("CRA") is based on the evaluation of a range of risk factors that may influence the level of money laundering and terrorist financing ("ML/FT") risk associated with a customer

The Company assess risk across four primary categories:

- customer risk
- geographical risk
- product, service and transaction risk
- delivery channel risk

Each category captures different dimensions of risk and is assessed using defined indicators and criteria, as further detailed in the sections below

The assessment of these risk factors is conducted in a holistic manner, taking into account both quantitative and qualitative considerations, and reflects the Company's overall risk-based approach

No single risk factor shall be considered in isolation. The overall risk rating assigned to customer risk determined based on the combined effect of all relevant factors

CUSTOMER RISK

Customer risk refers to the ML/FT/PF risk associated with the natural person based on person's economic activity and/or source of wealth.

Customer risk shall include consideration of:

- customers who have multiple sources of income;
- customers with irregular income streams
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);

GEOGRAPHICAL RISK

Geographical risk refers to the risk associated with the jurisdictions connected to the customer, its source funds, and source of wealth of the business relationship.

The Company shall assess geographical risk by considering all relevant jurisdictions linked to the customer, including:

- The nationality
- Residence address
- Place of birth

The Company shall consider, inter alia:

- 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 International Narcotics Control Strategy Report (INCSR);
- 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 AML/CFT regime;
- Countries sanctioned by OFAC
- Countries identified by credible sources as providing funding or support for terrorist activities or having terrorist organizations operating within them
- Countries on the Corruption Perception Index compiled by Transparency International

PRODUCT, SERVICE AND TRANSACTION RISK

Product, service and transaction risk arising from the gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others.

The Company shall assess the product, service and transaction risk by considering whether it may increase exposure to money laundering, terrorist financing or proliferation ("ML/FT/PF")

Particular consideration shall be given to:

- **Criminal Proceeds**- Funds deposited or wagered may originate from unlawful activities, including but not limited to fraud, payment card fraud, narcotics trafficking, theft, embezzlement, tax evasion or other criminal conduct
- **Anonymous or Pseudonymous Payment Methods**- the use of prepaid cards, virtual assets, cryptocurrencies, or other payment instruments that limit transparency may increase the risk of obscuring the source of funds or identify of the customer
- **Misuse of Gambling Accounts**- Customer accounts may be used primary as a vehicle for depositing and withdrawing funds with little or no genuine gambling activity, thereby facilitating the layering or integration of illicit proceeds
- **Low-Risk Betting Patterns**- Customers may place bets designed to minimize gambling risk, such as even-money wagers in roulette or similar games, with the intention of creating a legitimate audit trail for criminal funds

- **Peer-to-Peer Gaming Risks-** Games involving direct interaction and fund transfers between players may be vulnerable to collusion, chip dumping, or the transfer of illicit funds between accounts
- **Third-Party Funding-** The use of payment cards, bank accounts, e-wallets, or other financial instruments registered in the name of a third party may indicate an attempt to conceal the true source of funds
- **Transfers Between Gaming Accounts-** Internal transfers of funds between customer accounts may be used to move or disguise the origin and ownership of funds
- **Financial Service Abuse-** Services such as credit facilities, currency exchange, cheque cashing, or similar financial products may be exploited to facilitate money laundering activities
- **Multiple Accounts or Wallet Structures-** Customers operating multiple gaming accounts, wallets, or accounts related platforms may seek to circumvent controls, obscure transaction flows, or facilitate illicit activity
- **Frequent Changes to Funding Sources-** Repeated modifications to linked bank accounts, payment cards, e-wallets, or other payment method may indicate an attempt to avoid detection or conceal beneficial ownership
- **Identity Theft and Account Takeover Risks-** Stolen identities, compromised payment credentials, or fraudulently obtained financial accounts may be used to register, fund or operate gambling accounts
- **Prepaid Card Funding Risks-** The use of prepaid cards funded through cash or unverified sources may present similar ML/TF/PF risk to direct cash transactions
- **Shared Liquidity or Multi Operator Gaming Platforms-** Games hosted across shared networks or platforms involving multiple operators may create additional challenges in monitoring transactions and identifying suspicious activity
- **Electronic Wallet (E-Wallet)** – Certain e-wallet providers may operate in jurisdictions with weaker regulatory oversight or may permit funding methods that obscure the source of funds. In some cases, banking records may only reflect transfers to the e-wallet provider rather than the underlying gambling transactions potentially reducing transaction transparency and facilitating concealment of gambling activity

DELIVERY CHANNEL RISK

Delivery channel risk refers to the risk arising from the manner in which the Company establishes and maintains business relationship with a customer

The Company have identified the following delivery channel risk due to the nature of its business

- **Anonymous Delivery Channels-** Delivery channels that limit transparency regarding a customer's identity, source of funds, or transactional activity may increase the risk of ML/TF/PF. The Company shall implement appropriate customer due diligence, verification, and monitoring controls to mitigate risks associated with anonymity
- **Non-Face-to-Face Interaction-** The Company conducts business exclusively through remote channels, customer onboarding and interaction are performed on a non-face-to-face basis. This delivery method presents an increased risk of identity fraud, impersonation, and the use of falsified documentation. To mitigate these risks, the Company shall implement robust technological controls, including electronic identity verification, screening, and ongoing monitoring measures

7. TECHNOLOGICAL RISK ASSESSMENT

The Operator shall maintain appropriate policies, procedures, and controls to identify, assess, and mitigate money laundering and terrorist financing (ML/TF) risks arising from technological developments and innovation within its business operations

A Technology Risk Assessment shall be conducted whenever:

- A new product, game, or gaming service is introduced;
- A new business practice, operational process, or customer journey is implemented
- A new delivery channel or customer access mechanism becomes available;
- New or developing technologies are adopted in relation to existing or new products and services, including but not limited to payment solutions, identity verification tools, customer onboarding systems, artificial intelligence, automation tools, virtual assets, or other technology-driven solutions

Prior to implementation or launch, the Operator shall assess whether the proposed product, service, process, or technology introduces vulnerabilities that could be exploited for money laundering, terrorist financing, fraud, identity theft, sanctions evasion, or other financial crime purposes

The assessment shall consider, where applicable:

- The impact on customer identification and verification process;
- The ability to monitor and detect suspicious activity;
- The transparency of transactions and source of funds information;
- The involvement of third-party service providers
- Data security, cybersecurity and account takeover risks
- The potential for anonymity, concealment of beneficial ownership, or circumvention of existing AML/CFT controls
- Regulatory and compliance obligations associated with the technology

All Technology Risk Assessments shall be documented and retained in accordance with the Operator's record-keeping requirements. Where risks are identified, appropriate mitigating controls shall be implemented prior to deployment. Such controls may include enhanced customer due diligence measures, additional transaction monitoring rules, system restrictions, enhanced screening procedures, staff training or other risk-based controls deemed necessary by the Operator

The Compliance Function, in coordination with relevant business and technology stakeholders, shall review and approve the assessment before the relevant product, service, process or technology is introduced into the operational environment

8. CUSTOMER ONBOARDING AND DUE DILIGENCE

The Company applies a risk-based approach to customer onboarding, ensuring that no business relationship is established until the money laundering and terrorist financing ("ML/TF") risks associated with the customer have been appropriately identified, assessed, and mitigated

Customer onboarding is conducted in accordance with the outcome of the Customer Risk Assessment ("CRA") and the Company's defined risk appetite, as set out in Section 5.4 of this Policy.

As part of the onboarding process, the Company shall apply Customer Due Diligence ("CDD") measures to:

- Identify and verify the identity of the customer
- Assess the purpose and intended nature of the business relationship; and
- Determine whether the level of risk presented is acceptable within the Company's risk appetite

The nature and extent of the due diligence measures shall be proportionate to the level of risk identified with enhanced measures applied only where permitted and justified

The Company shall not establish or continue a business relationship where it is unable to adequately identify and verify the customer or where the ML/FT risks cannot be effectively mitigated

Further details on client acceptance, due diligence measures, and enhanced controls are set out in the sections below.

8.1 CUSTOMER ACCEPTANCE

The Company adopts a risk-based approach to client acceptance and shall only establish or maintain business relationships which are considered consistent with the Company's risk appetite and AML/CFT framework

Client acceptance decisions shall be based on the outcome of the Customer Risk Assessment ("CRA") and the application of appropriate Customer Due Diligence ("CDD") measures

Prior to onboarding, the Company shall obtain sufficient information to:

- Identify and verify the identity of the customer
- understand the purpose and intended nature of the business relationship; and
- assess the customer's ML/FT risk profile

The Company shall not establish or continue a business relationship where:

- required CDD measures cannot be completed
- the information or documentation provided appears false, misleading, inconsistent or unreliable
- the customer seeks to establish a relationship using anonymous, fictitious or false identifies or
- the relationship falls outside the Company's risk appetite or applicable legal and regulatory requirements

Where a business relationship is declined or terminated, the rationale shall be appropriately documented and escalated internally where necessary

8.2 CUSTOMER DUE DILIGENCE (CDD)

The Company shall apply Customer Due Diligence ("CDD") measures in accordance with a risk-based approach to identify and verify customers and Ultimate Beneficial Owner(s) ("UBOs"), and to understand the nature and purpose of the business relationship.

CDD measures shall be applied:

- prior to the establishment of a business relationship or the carrying out of an occasional transaction;

- where there is knowledge, suspicion, or reasonable grounds to suspect money laundering or terrorist financing (“ML/FT”);
- where doubts arise regarding previously obtained customer information or documentation;
- and on an ongoing basis throughout the business relationship.

As part of the CDD process, the Company shall:

- identify and verify the customer using reliable and independent documentation or information;
- identify and verify the UBO(s) and understand the ownership and control structure;
- obtain information regarding the purpose and intended nature of the relationship; and
- conduct ongoing monitoring to ensure that customer information remains accurate and up to date.

CDD measures shall be applied on a risk-sensitive basis and shall be proportionate to the customer’s ML/FT risk profile.

Enhanced Due Diligence (“EDD”) measures shall be applied in higher-risk situations, while Simplified Due Diligence (“SDD”) may only be applied where permitted by applicable legal and regulatory requirements.

Where the Company is unable to complete required CDD measures, the relationship shall not proceed or shall be terminated, as appropriate

8.3 SIMPLIFIED DUE DILIGENCE (SDD)

The Company may apply Simplified Due Diligence (“SDD”) measures where it has determined, through its Customer Risk Assessment, that a customer presents a lower risk of money laundering, terrorist financing, or proliferation financing.

The application of SDD shall be risk-based and shall not exempt the Company from its obligation to identify customers, conduct ongoing monitoring, or detect unusual or suspicious activity.

Customers may only be classified as low risk where there are no higher-risk indicators present and the Company is satisfied that the customer relationship presents a reduced ML/TF/PF risk.

A. Simplified Due Diligence Measures

Where a customer is assessed as low risk, the Company may apply one or more of the following measures:

- Limit customer identification requirements to the minimum onboarding information required under this Policy;
- Apply a reduced level of verification where permitted by applicable laws and regulations;
- Utilize reliable electronic verification tools and alternative independent data sources to verify customer information;
- Reduce the frequency of periodic customer reviews;
- Apply standard transaction monitoring commensurate with the customer's risk profile;
- Request Source of Funds or Source of Wealth information only where triggered by transaction thresholds, unusual activity, or other risk indicators; and
- Apply other proportionate measures deemed appropriate based on the customer's risk profile.

The Company shall maintain sufficient information and documentation to ensure it has a reasonable understanding of the customer's identity, activity, and risk profile at all times.

B. Ongoing Monitoring of Low-Risk Customers

Customers classified as low risk shall remain subject to ongoing transaction and activity monitoring throughout the business relationship.

The Company shall ensure that customer activity remains consistent with the customer's known profile and expected gambling behaviour and shall investigate any unusual, unexpected, or potentially suspicious activity regardless of the customer's risk classification.

C. Restrictions on the Use of Simplified Due Diligence

Simplified Due Diligence shall not be applied where:

- There is knowledge, suspicion, or reasonable grounds to suspect money laundering, terrorist financing, or proliferation financing;
- The customer is identified as a Politically Exposed Person ("PEP"), family member, or close associate of a PEP;
- The customer is subject to sanctions screening alerts;
- The customer is connected to a higher-risk jurisdiction;
- Adverse media or other negative information has been identified;
- Enhanced Due Diligence requirements have been triggered;
- The customer's activity is inconsistent with their known profile;
- Source of Funds or Source of Wealth concerns have been identified; or
- Any other higher-risk factors exist that warrant additional due diligence measures.

8.4 ENHANCED DUE DILIGENCE (EDD)

The Company shall apply Enhanced Due Diligence ("EDD") measures where a customer, transaction, product, geographic location, or activity presents a higher risk of money laundering, terrorist financing, or proliferation financing.

EDD measures shall be proportionate to the level and nature of the risk identified and shall supplement the standard Customer Due Diligence requirements set out in this Policy.

The objective of EDD is to obtain a greater understanding of the customer, the source of funds and source of wealth, and the purpose of transactions, while increasing the level of monitoring applied to the business relationship.

A. Enhanced Due Diligence Triggers

EDD may be applied in circumstances including, but not limited to:

- Customers identified as Politically Exposed Persons ("PEPs"), their family members, or close associates;
- Customers residing in, transacting from, or otherwise connected to higher-risk jurisdictions;
- Customers exhibiting unusual or complex transaction patterns;
- Customers conducting high-value or high-volume gambling activity;

- Customers whose activity is inconsistent with their known profile, source of funds, or source of wealth;
- Customers generating adverse media alerts or negative intelligence;
- Customers using products, services, technologies, or payment methods that increase anonymity risks;
- Customers suspected of acting on behalf of third parties;
- Customers triggering multiple AML monitoring alerts; or
- Any other circumstance assessed by the Company as presenting an elevated ML/TF/PF risk.

B. Enhanced Due Diligence Measures

Depending on the risk identified, the Company may apply one or more of the following measures:

- Obtain additional information regarding the customer's identity, occupation, employment, business activities, or financial circumstances;
- Obtain additional information regarding the intended nature and purpose of the business relationship;
- Obtain Source of Funds ("SOF") information and supporting documentation;
- Obtain Source of Wealth ("SOW") information and supporting documentation;
- Request documentation supporting specific transactions, deposits, or withdrawals;
- Verify ownership of payment methods and financial accounts used by the customer;
- Conduct enhanced open-source, adverse media, and intelligence checks;
- Obtain additional documentation to verify information provided by the customer;
- Increase the frequency of customer reviews and risk reassessments;
- Apply enhanced transaction and activity monitoring; and
- Implement any additional controls deemed necessary to mitigate the identified risks.

Examples of acceptable Source of Funds and Source of Wealth documentation may include:

- Payslips or employment contracts;
- Bank statements;
- Tax returns;
- Business ownership records;
- Investment or dividend statements;
- Property sale documentation;
- Inheritance documentation;
- Legal settlement documentation; or
- Other reliable evidence demonstrating the legitimate origin of funds or wealth.

C. Enhanced Monitoring

Customers subject to EDD shall be subject to increased monitoring throughout the business relationship.

Enhanced monitoring may include:

- Increased scrutiny of deposits, withdrawals, and wagering activity;
- More frequent review of customer transactions and behavioural patterns;
- Periodic refresh of Source of Funds and Source of Wealth information;
- More frequent sanctions, PEP, and adverse media screening;
- Review of payment methods and funding sources; and

- Additional investigation of unusual or suspicious activity.

The Company may request updated Source of Funds or Source of Wealth information at any time where the customer's risk profile, transaction activity, or other risk indicators warrant additional review, regardless of whether there has been a material change in account activity.

D. Review and Escalation

Customers subject to Enhanced Due Diligence shall be reviewed more frequently than standard-risk customers in accordance with the Company's risk-based review schedule.

Where the Company is unable to obtain sufficient information to mitigate identified risks, or where concerns regarding the legitimacy of funds, wealth, or customer activity remain unresolved, the matter shall be escalated to the MLRO for further assessment.

The Company may restrict, suspend, or terminate the business relationship where adequate due diligence cannot be completed or where the risks cannot be effectively managed.

Any suspicious activity identified during the Enhanced Due Diligence process shall be assessed for potential reporting to the FIU Curaçao in accordance with applicable legal and regulatory requirements.

9. CDD MEASURES

The Company shall apply Customer Due Diligence ("CDD") measures in accordance with a risk-based approach to identify and verify customers and to understand the nature and purpose of the business relationship

CDD measures shall be applied or conducted in the following circumstances:

- when customer engages in financial transactions equal to or exceeding NAF 4,000 (or the equivalent amount in another currency);
- when carrying out an occasional transaction equal to or exceeding NAF 4,000 (or the equivalent amount in another currency);
- where there is a knowledge, suspicion, or reasonable grounds to suspect money laundering or terrorist financing ("ML/FT")
- where doubts arise regarding previously obtained customer information or documentation

The Company shall aggregate linked or related transactions conducted by the same customer, account, device, payment instrument, or gaming session to determine whether the applicable threshold has been reached. Where multiple transactions appear connected and cumulatively meet or exceed the threshold of NAF 4,000, the Company shall apply the required CDD measures irrespective of the value of the individual transactions

At a minimum, the CDD measures shall include;

- Customer Identification and Verification

The Company shall identify each customer and verify their identity using reliable and independent documentation, data, or information. Verification shall be completed through approved electronic verification tools, government-issued identification documents, proof of address documentation where required, and any other verification methods deemed appropriate based on customer's risk profile

At a minimum, the following information must be collected from the customers;

i. full name

ii. permanent residential address

- Beneficial Ownership and Verification

Where the customer is a legal entity, trust, partnership or other legal arrangement, the Company shall identify the ultimate beneficial owner(s) and take reasonable measures to verify their identity. The Company shall obtain sufficient information to understand the ownership and control structure of the customer and determine the natural person(s) who ultimately own, control, or benefit from the business relationship

- Purpose and Intended Nature of the Business Relationship

The Company shall obtain and assess information necessary to understand the purpose and intended nature of the customer relationship. This may include information relating to the following;

a. customer's occupation

b. source of funds

c. expected level of gambling activity

d. payment methods

e. geographic connections

10. BENEFICIAL OWNERSHIP

As a business-to-consumer ("B2C") online gambling operator, the Company only permits natural persons to register and operate customer accounts. Corporate entities, partnerships, trusts, and other legal arrangements are not permitted to establish customer accounts or participate in gambling activities through the Company's platform.

The Company shall take reasonable measures to ensure that each customer is acting on their own behalf and for their own benefit when establishing and maintaining a business relationship.

During the onboarding process, customers shall be required to confirm that:

- The account is being opened in their own name;
- They are the beneficial owner of the account;
- They are using their own funds for gambling activities; and
- They are not acting on behalf of, or under the instruction of, any third party.

Such confirmations may be obtained through customer declarations, acceptance of the Terms and Conditions, account registration processes, or other controls implemented by the Company.

The Company shall not rely solely on customer declarations and shall maintain appropriate controls designed to identify circumstances where a customer may be acting on behalf of another individual or group of individuals.

10.1 IDENTIFICATION

The Company shall obtain sufficient customer information to establish the identity of each customer prior to establishing a business relationship permitting gambling activity where required, or conducting transactions that trigger CDD obligations

As a minimum, the following shall be collected

- Full legal name
- Residential address
- Date of birth
- Place of birth
- Nationality; and
- Government-issued identification number

For customers assessed as presenting a lower ML/TF/PF risk, the Company may limit the initial identification requirements to the customer's full name, residential address, and date of birth, where permitted by applicable laws and regulations

For customers assessed as presenting a higher ML/TF/PF risk, the Company may obtain additional information and documentation, including but not limited to occupation, source of funds, source of wealth, tax residence, payment instrument ownership, and other information necessary to adequately mitigate the identified risk

Where customer accounts can be used for both free-play and real money gambling activities, customer identification requirements shall be applied before the customer permitted to participate in real-money gambling activities or otherwise in accordance with applicable regulatory requirements

10.2 VERIFICATION

The Company shall verify the identity of customers using reliable and independent documentation, data, or information.

As a standard requirement, identity verification shall be completed through the review of a valid, unexpired government-issued identification document containing the customer's photograph, such as:

- Passport;
- National identity card; or
- Driver's licence, where acceptable under applicable procedures.

Where the identification document does not verify the customer's residential address, the Company may request additional supporting documentation, including:

- Bank statements;
- Utility bills;
- Government correspondence;

- Tax documentation;
- Rental or tenancy agreements; or
- Other reliable proof of address documents.

At a minimum, proof of address documentation should generally be dated within the previous six (6) months

The Company shall not establish or continue a business relationship where customer identity cannot be satisfactorily verified.

10.3 PURPOSE AND INTENDED NATURE OF BUSINESS

The Company shall obtain sufficient information to understand the purpose and intended nature of the business relationship and to develop an appropriate customer risk profile. This information shall enable the Company to assess whether a customer's activity is consistent with their known profile and to identify unusual or potentially suspicious activity throughout the customer lifecycle.

Given the nature of the Company's business as an online gambling operator, the primary purpose of the business relationship is generally self-evident, namely the customer's participation in online gambling activities offered through the Company's platform. Accordingly, customers are not ordinarily required to provide a detailed explanation regarding the purpose of opening a gaming account.

Notwithstanding the above, the Company shall collect sufficient information to establish an expected customer profile and assess the legitimacy of the customer's gambling activity, taking into consideration the customer's risk rating and anticipated level of activity.

10.4 POLITICALLY EXPOSED PERSON (PEPS)

Politically Exposed Persons ("PEPs") are individuals who are or have been entrusted with prominent public functions and, by virtue of their position and influence, may present a higher risk of money laundering and terrorist financing ("ML/FT").

The Company shall identify whether a customer, its Ultimate Beneficial Owner(s) ("UBOs"), or any related party is a PEP, or a family member or known close associate of a PEP, as part of the Customer Due Diligence ("CDD") process and on an ongoing basis.

The Company shall identify PEPs through a combination of:

- internal screening systems and commercial databases;
- open-source intelligence (including reputable media searches); and
- customer declarations and information obtained during onboarding and ongoing monitoring.

10.4.1 ENHANCED DUE DILIGENCE FOR PEP

Where a customer, UBO, or related party is identified as a PEP, the Company shall apply Enhanced Due Diligence ("EDD") measures in accordance with Section 7.4 of this Policy.

Such measures shall include, at a minimum:

- obtaining information on, and where appropriate verifying, the source of wealth and source of funds;

- conducting enhanced and more frequent ongoing monitoring of the relationship; and
- applying increased scrutiny to transactions and the overall relationship.

10.4.2 SENIOR MANAGEMENT APPROVAL

The establishment or continuation of a business relationship with a PEP shall require prior approval from Senior Management.

Decisions relating to the acceptance, continuation, or termination of relationships involving PEPs shall be appropriately documented, including the rationale for the decision and any mitigating measures applied.

10.5 SANCTIONS SCREENING

The Company shall implement and maintain effective sanctions screening controls to ensure compliance with applicable restrictive measures and sanctions regimes.

Sanctions screening shall be conducted in respect of customers, Ultimate Beneficial Owner(s) ("UBOs"), authorised signatories, and, where relevant, counterparties and transactions.

Screening shall be performed:

- prior to the establishment of a business relationship or the execution of an occasional transaction;
- on a periodic basis throughout the course of the business relationship;
- without undue delay upon the occurrence of any trigger event (including changes in ownership, control, or customer profile); and
- on a real-time or near real-time basis where transactions or activities are carried out.

The Company shall screen against, at a minimum:

- United Nations sanctions lists;
- European Union consolidated sanctions list;
- Any Curaçao sanctions or designated persons lists, where applicable;

Where the Company identifies or **confirms** that a customer or other relevant party is a designated person or entity under applicable sanctions legislation, the Company shall immediately take appropriate action in accordance with applicable legal and regulatory requirements. Such measures may include:

- restricting or suspending the customer account;
- prohibiting deposits, withdrawals, transfers, or any other transactions involving the customer;
- implementing an asset freeze where required by applicable sanctions legislation;
- ensuring that no funds, assets, or economic resources are made available, directly or indirectly, to or for the benefit of a designated person or entity except where authorised by law;
- escalating the matter immediately to the MLRO for assessment and determination of any applicable reporting or notification obligations; and
- complying with any freezing order, direction, licence, or instruction issued by a competent authority.

The Company shall not establish or maintain a business relationship with any customer who is subject to applicable sanctions or whose activity would result in a breach of sanctions obligations.

Employees shall maintain strict confidentiality in relation to sanctions investigations and shall not disclose the existence of a sanctions review, asset freezing measure, or related investigation to the customer or any unauthorised person, except where disclosure is authorised or required by applicable law

11. ONGOING MONITORING REVIEW

The Company shall conduct ongoing monitoring of the customer relationship and review transactions, deposits, withdrawals, gameplay activity, and other relevant account activity to ensure that such activity remains consistent with the customer's known profile, risk rating, and expected behaviour. Where necessary, the Company shall obtain additional information regarding the customer's source of funds, source of wealth, or the rationale of specific transactions

The Company shall maintain up-to-date customer records and periodically review customer information based on the customer's risk classification. Any unusual, inconsistent, or potentially suspicious activity identified through ongoing monitoring shall be escalated to the MLRO for review and consideration of further action including the filing of a report with the FIU Curacao where required

11.2 TRIGGER EVENTS

The Company shall maintain appropriate monitoring controls to identify transaction and customer activity patterns that may indicate increased money laundering, terrorist financing, proliferation financing, fraud, or other financial crime risks.

The occurrence of one or more trigger events shall result in an appropriate review of the customer relationship and, where necessary, the application of additional due diligence measures, source of funds verification, enhanced monitoring, account restrictions, escalation to the MLRO, and/or reporting to the FIU Curaçao.

Transaction Trigger Events

The following transaction-related events may trigger additional review:

- Single deposits or withdrawals exceeding internally established AML review thresholds.
- Cumulative deposits or withdrawals exceeding predefined monitoring thresholds within a specified period.
- Significant increases in deposit or withdrawal activity compared to the customer's historical transaction patterns.
- Rapid deposits followed by withdrawal requests with little or no gambling activity.
- Multiple deposits or withdrawals conducted within a short period of time.
- Frequent deposits followed by minimal-risk wagering activity.
- Use of multiple payment methods without a reasonable explanation.
- Deposits made using payment methods registered to third parties.
- Frequent changes to payment methods, banking details, or withdrawal destinations.
- Repeated failed deposit attempts followed by successful transactions through alternative payment methods.
- Transactions involving higher-risk jurisdictions.
- Transactions that appear structured to avoid internal review thresholds or regulatory requirements.

- Transactions inconsistent with the customer's known source of funds, source of wealth, or financial profile.
- Unusual payment flows that lack an apparent economic purpose.
- Any transaction giving rise to knowledge, suspicion, or reasonable grounds to suspect money laundering, terrorist financing, proliferation financing, or other criminal activity.

Customer Activity Trigger Events

The following customer activity-related events may trigger additional review:

- Significant increases in gambling activity compared to the customer's historical behaviour.
- Sudden movement from low-value to high-value gambling activity.
- Gambling activity inconsistent with the customer's known profile, occupation, source of funds, or source of wealth.
- Sustained high-volume wagering activity.
- Unusual betting patterns or gameplay behaviour that deviate from expected customer activity.
- Minimal-risk betting strategies designed primarily to move funds rather than participate in gambling.
- Patterns indicative of account sharing, account takeover, or operation by multiple individuals.
- Indicators of syndicate betting or coordinated gambling activity.
- Use of VPNs, proxies, anonymisation tools, or other methods intended to conceal customer identity or location.
- Multiple customer accounts linked through common devices, IP addresses, payment methods, contact details, or other identifying information.
- Repeated attempts to circumvent account restrictions, responsible gambling controls, or verification requirements.
- Significant discrepancies between customer declarations and actual account activity.
- Refusal, delay, or reluctance to provide requested CDD, Source of Funds, or Source of Wealth information.
- Adverse media, sanctions alerts, PEP identification, or other information that materially changes the customer's risk profile.
- Activity inconsistent with the customer's expected behavioural profile or risk rating.
- Any behaviour that appears unusual, suspicious, or indicative of potential money laundering, terrorist financing, proliferation financing, fraud, or other criminal conduct.

11.3 REVIEW FREQUENCY

The Company shall conduct periodic reviews of customer relationships to ensure that customer information, risk ratings, and due diligence records remain accurate, complete, and up to date.

The minimum review frequency shall be based on the customer's current risk classification:

Risk Level	Minimum Review Frequency
Low	Triggered events
Medium	Every 6 months
High	Every 3 months

11.4 MONITORING MEASURES

Where one or more trigger events are identified, the Company shall conduct a risk-based review to determine whether additional information, documentation, or due diligence measures are required.

Depending on the nature and severity of the trigger event, the Company may:

- Request additional customer information or documentation;
- Conduct Source of Funds or Source of Wealth verification;
- Apply Enhanced Due Diligence measures;
- Increase the frequency and intensity of ongoing monitoring;
- Restrict, suspend, or terminate the customer relationship;
- Escalate the matter to the MLRO for further investigation; and/or
- Submit a report to the FIU Curaçao where required by law.

11.5 TIMING OF CDD MEASURES

The Company shall apply Customer Due Diligence ("CDD") measures at onboarding, throughout the customer relationship, and whenever regulatory thresholds, trigger events, or higher-risk circumstances arise.

A. Account Registration

Upon account registration, and prior to permitting gambling activity where required, the Company shall collect, at a minimum:

- Full name;
- Residential address;
- Date of birth; and
- Any other information required to comply with applicable legal and regulatory obligations.

The Company shall also perform sanctions screening and Politically Exposed Person ("PEP") screening as part of the onboarding process.

B. Threshold-Based CDD

The Company shall monitor customer transactions on an ongoing basis and calculate cumulative financial transactions from the commencement of the business relationship.

Where a customer reaches or exceeds the cumulative threshold of NAf. 4,000 (or the equivalent in another currency), the Company shall complete the remaining CDD requirements, including:

- Verification of customer identity;

- Customer Risk Assessment ("CRA");
- Additional due diligence measures where required; and
- Any other information necessary to satisfy the Company's AML/CFT obligations.

The Company may apply these measures before the threshold is reached where required by the customer's risk profile, transaction activity, or other risk indicators.

C. Account Restrictions Pending CDD Completion

Where additional CDD information or documentation is required, the customer may continue to access their account subject to the restrictions determined by the Company.

Where the applicable threshold has been reached and CDD remains incomplete, the Company may restrict deposits, withdrawals, or other account functionality until the required information has been obtained and verified.

The nature and extent of any restrictions shall be determined on a risk-based basis and in accordance with the Company's AML/CFT procedures.

D. Failure to Complete CDD

Customers shall be required to provide all requested information and documentation within thirty (30) days of the Company's request, unless a shorter period is deemed appropriate based on the circumstances.

Where a customer fails to provide the required information within the prescribed timeframe, the Company shall:

- Restrict or suspend the customer account as appropriate;
- Consider termination of the business relationship;
- Conduct an assessment of any ML/TF/PF risks identified; and
- Escalate the matter to the MLRO where necessary.

Where suspicion of money laundering, terrorist financing, or proliferation financing exists, the MLRO shall determine whether a report should be submitted to the FIU Curaçao in accordance with applicable legal requirements.

E. Trigger-Based Reviews

The Company shall not rely solely on monetary thresholds when determining when CDD measures are required.

Additional CDD, Enhanced Due Diligence, Source of Funds, Source of Wealth, or customer risk reviews may be triggered at any time where:

- Unusual or suspicious activity is identified;
- Transaction or activity trigger events occur;

- The customer's risk profile changes;
- Sanctions, PEP, or adverse media alerts are identified; or
- The Company otherwise determines that additional due diligence is necessary to manage ML/TF/PF risk.

12. SUSPICIOUS ACTIVITY/TRANSACTION REPORTING (SAR/STR)

The Company shall implement and maintain effective procedures for the identification, internal reporting, assessment, and external reporting of suspicious activity, in accordance with applicable AML/CFT laws and regulations.

All Personnel shall remain vigilant to indicators of money laundering or terrorist financing (“ML/FT”) and shall promptly report any knowledge, suspicion, or reasonable grounds to suspect ML/FT to the Money Laundering Reporting Officer (“MLRO”) without delay

An unusual transaction is a transaction inconsistent with the player’s profile. The following transactions or intended transactions are deemed unusual and are the following but not limited to;

A. Suspicious Transactions

- Significant deposits or withdrawals inconsistent with the customer's known profile or expected activity.
- Sudden increases in deposit, wagering, or withdrawal activity.
- Rapid deposits followed by withdrawals with little or no gambling activity.
- Frequent deposits followed by minimal-risk wagering activity.
- Multiple deposits or withdrawals conducted within a short period of time.
- Transactions structured to avoid internal monitoring thresholds or regulatory reporting requirements.
- Use of multiple payment methods without a reasonable explanation.
- Frequent changes to payment methods, withdrawal destinations, or banking details.
- Deposits or withdrawals involving third-party payment methods.
- Transactions involving higher-risk jurisdictions or unusual payment flows.
- Transactions lacking an apparent economic or lawful purpose.

B. Suspicious Activity

- Gambling activity inconsistent with the customer's known profile, source of funds, or source of wealth.
- Significant changes in gambling behaviour without a reasonable explanation.
- Unusually high wagering volumes or turnover.
- Sudden transition from low-value to high-value gambling activity.
- Patterns of activity inconsistent with the customer's historical behaviour.
- Repeated attempts to circumvent account limits, verification requirements, or other controls.
- Activity inconsistent with the customer's declared occupation, income level, or financial circumstances.
- Behaviour suggesting that gambling activity is being used primarily to transfer, move, or disguise funds.

The presence of one or more indicators does not automatically mean that money laundering, terrorist financing, or other criminal activity has occurred. However, such indicators shall trigger an appropriate review and, where necessary, escalation to the MLRO for further assessment.

12.1 INTERNAL REPORTING

Where Personnel know, suspect, or have reasonable grounds to suspect that funds or activities may be linked to ML/FT, they shall:

- submit an internal suspicious activity report to the MLRO as soon as practicable; and
- provide all relevant information and supporting documentation available.

Internal reports shall be treated as strictly confidential and shall be documented and retained in accordance with the Company's record-keeping obligations.

12.2 EXTERNAL REPORTING

Where the MLRO determines that there are reasonable grounds for suspicion, a report shall be submitted promptly to the competent authority, in accordance with applicable legal and regulatory requirements.

The Company shall ensure that such reporting is carried out without undue delay and that all relevant information is included in the report

12.3 NO TIPPING OFF

Personnel shall not disclose to the customer or any third party that:

- a suspicion has been formed;
- an internal report has been made; or
- a report has been submitted to a competent authority.

Any breach of this prohibition may constitute a criminal offence and shall be subject to disciplinary action.

13. TERMINATION OF BUSINESS RELATIONSHIP

The Company shall not establish or continue a business relationship where it is unable to comply with its Customer Due Diligence ("CDD") obligations or where the risks associated with the customer relationship cannot be adequately managed.

The Company may restrict, suspend, or terminate a customer relationship where:

- Required CDD information or documentation is not provided within 30 days timeframe;
- Customer identity cannot be satisfactorily verified;
- Source of Funds ("SOF") or Source of Wealth ("SOW") requirements cannot be fulfilled where required;
- The customer refuses to cooperate with CDD, EDD, or ongoing monitoring requirements;
- The customer provides false, misleading, incomplete, or inconsistent information;
- The Company is unable to adequately mitigate identified ML/TF/PF risks; or

- Continued operation of the account would expose the Company to unacceptable regulatory, legal, financial crime, or reputational risk.

13.1 ACCOUNT RESTRICTION AND SUSPENSION

Where outstanding CDD requirements remain unresolved, the Company may apply account restrictions pending completion of the required verification measures.

Such restrictions may include:

- Prohibiting deposits;
- Restricting withdrawals;
- Suspending gambling activity;
- Temporarily blocking account access; or
- Applying any other control considered necessary to mitigate identified risks.

The nature and extent of restrictions shall be proportionate to the circumstances and risk presented by the customer.

13.2 TERMINATION DECISION

Prior to terminating a customer relationship, the Company shall review the circumstances surrounding the case and consider:

- The customer's risk profile;
- The nature of the outstanding information or documentation;
- The customer's level of cooperation;
- Any unusual or suspicious activity identified;
- Any legal, regulatory, or compliance concerns; and
- Any other relevant risk indicators.

The Company shall retain records relating to account restrictions, suspensions, terminations, customer communications, supporting documentation, and decisions taken in connection with the termination of the business relationship in accordance with its record-keeping obligations.

13.3 RETURN OF CUSTOMER FUNDS

Where the business relationship is terminated and there are no legal, regulatory, or AML/CFT grounds preventing the return of customer funds, any eligible balance shall be returned through the same payment method or funding source originally used by the customer, where operationally feasible.

Prior to returning funds, the Company shall ensure that:

- Applicable AML/CFT requirements have been considered;
- No legal or regulatory restrictions apply; and
- No outstanding concerns exist that would prevent the return of funds.

Where AML/CFT concerns have been identified, the handling of customer funds shall be determined in accordance with applicable laws, regulatory requirements, and the Company's internal procedures.

14. TRAINING

The Company shall implement and maintain effective measures to ensure that all Personnel are appropriately trained, competent, and fit to perform their functions in relation to Anti-Money Laundering and Counter-Financing of Terrorism (“AML/CFT”) obligations.

The Company shall promote a strong culture of AML/CFT compliance and risk awareness across all levels of the organisation.

All Personnel, including those based outside Curacao where relevant to the Company’s operations, shall receive AML/CFT training:

- upon commencement of their engagement; and
- at least annually thereafter, or more frequently where required.

Training programmes shall be tailored to the role and responsibilities of the individual and shall ensure that Personnel are able to:

- recognise indicators of money laundering and terrorist financing (“ML/FT”);
- understand the Company’s AML/CFT policies and procedures;
- identify and escalate suspicious activity in accordance with Section 10 of this Policy; and
- understand their legal and regulatory obligations.

Enhanced and role-specific training shall be provided to Personnel with higher AML/CFT responsibilities, including:

- client-facing Personnel;
- members of the Compliance and Risk functions;
- the Money Laundering Reporting Officer (“MLRO”) and support staff;
- Senior Management; and
- members of the Board of Directors.

Such training shall include, where relevant, detailed instruction on Suspicious Transaction Reporting (“STR”) and Suspicious Activity Reporting (“SAR”), risk assessment, and ongoing monitoring obligations.

14.1 PERSONNEL VETTING

The Company shall implement and maintain appropriate procedures to assess the integrity, competence, and suitability of Personnel who perform, or are in a position to influence, AML/CFT-relevant functions.

Personnel vetting shall be conducted on a risk-based and proportionate basis and shall include, where appropriate:

- verification of identity and relevant qualifications;
- assessment of experience and competence for the role;
- background checks to assess honesty, integrity, and reputation; and
- obtaining a police conduct certificate or equivalent documentation, where required or appropriate.

The Company shall ensure that Personnel are fit and proper to perform their functions and that any identified risks are appropriately mitigated.

Vetting shall be performed prior to engagement and may be repeated periodically or where circumstances warrant (e.g. change in role, emergence of adverse information, or regulatory requirements).

15. RECORD KEEPING

The Company shall maintain and retain adequate records to demonstrate compliance with its Anti-Money Laundering and Counter-Financing of Terrorism (“AML/CFT”) obligations and to enable the reconstruction of business relationships and activities where required.

Records shall be complete, accurate, and maintained in a manner that allows for their prompt retrieval without undue delay.

15.1 RECORDS MAINTAINED

The Company shall maintain, at a minimum, the following categories of records:

Risk-Based Approach Documentation

- the Business Risk Assessment (“BRA”);
- this AML/CFT Policy and any related procedures; and
- Customer Risk Assessments (“CRA”) carried out in respect of customers.

Customer Due Diligence (CDD) Records

Records relating to the identification and verification of customers and Ultimate Beneficial Owner(s) (“UBOs”), including:

- original documents or certified true copies, signed and dated where applicable;
- electronic copies retained and maintained in the Company’s systems;
- results of searches conducted using commercial electronic databases or other independent sources;
- records of video identification or verification processes (where applicable); and
- documentation used to verify residential address and other identifying information.

Business Relationship and Transaction Records

- client application forms and onboarding documentation;
- engagement letters and contractual agreements;
- invoices, payment confirmations, and other financial records (where applicable).

Monitoring, Screening, and Reporting Records

- records of ongoing monitoring activities, including periodic and event-driven reviews;
- sanctions screening and Politically Exposed Person (“PEP”) screening results;
- internal reports submitted to the Money Laundering Reporting Officer (“MLRO”);
- written records of decisions where a Suspicious Transaction Report (“STR”) or Suspicious Activity Report (“SAR”) was not submitted;
- STRs/SARs submitted to the Financial Intelligence Unit and any related correspondence or follow-up submissions;
- records of AML/CFT training provided to Personnel and attendance records;

- records of personnel vetting, including police conduct certificates or equivalent documentation (where applicable);
- records relating to outsourcing arrangements relevant to AML/CFT functions;
- reports submitted by the MLRO to Senior Management; and
- records of Senior Management's consideration, decisions, and actions.

Beneficial Ownership Documentation

The Company shall retain documentation evidencing:

- the steps taken to identify and verify beneficial ownership; and
- the rationale for determining beneficial ownership, including cases where senior managing officials are identified as beneficial owners.

General Requirement

Records shall be maintained in a manner that enables the reconstruction of business relationships and activities; and the provision of evidence for the investigation and prosecution of criminal activity.

15.2 RETENTION PERIOD

The Company shall retain all records obtained for the purposes of Anti-Money Laundering and Counter-Financing of Terrorism ("AML/CFT") compliance for a minimum period of **five (5) years**.

The retention period shall commence from either the date on which the business relationship with the customer has ended; or the date of the occasional transaction, as applicable.

Where required by the Financial Intelligence Analysis Unit, the supervisory authority, or any competent law enforcement agency, the Company shall extend the retention period beyond five (5) years, provided that the total retention period shall not exceed **ten (10) years**, unless otherwise required by applicable law.

Where the Company ceases to carry out relevant financial business or activities, its record-keeping obligations shall continue to apply until the applicable retention periods have fully lapsed.

The Company shall also ensure compliance with any longer retention requirements arising under other applicable legal or regulatory frameworks, including data protection and corporate governance obligations.

Upon expiry of the applicable retention period, records shall be securely deleted or anonymised, unless further retention is required by law.

16. INDEPENDENT AUDIT FUNCTION

The Company shall maintain an independent Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing ("AML/CFT/CPF") audit function to assess the adequacy, effectiveness, and ongoing compliance of its AML/CFT/CPF framework with applicable laws, regulations, regulatory guidance, and internal policies and procedures.

An independent AML/CFT audit shall be conducted at least annually by either the Company's Internal Audit function or an appropriately qualified independent external party. The audit shall be performed by individuals who are independent of the Company's AML/CFT compliance function and who possess the necessary knowledge, experience, and competence to evaluate the effectiveness of the Company's AML/CFT/CPF programme.

The independent audit shall adopt a risk-based approach and, at a minimum, assess the adequacy and effectiveness of the Company's:

- AML/CFT/CPF policies, procedures, manuals, and internal controls;
- Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), and ongoing monitoring processes;
- Customer files and supporting documentation to assess compliance with applicable customer identification and verification requirements;
- Transaction monitoring arrangements, including the identification, investigation, escalation, and reporting of unusual or suspicious activities;
- Compliance with applicable AML/CFT/CPF laws, regulations, regulatory guidance, and internal policies;
- Sanctions screening, politically exposed person (PEP) screening, and other customer screening controls;
- Employee AML/CFT training programme, including its adequacy, effectiveness, and record keeping;
- Record retention practices to ensure compliance with applicable legal and regulatory retention requirements;
- Systems, controls, and monitoring tools designed to detect unusual or suspicious customer activity; and
- Governance arrangements, including the effectiveness of AML oversight, reporting lines, and management supervision.

As part of the audit, the auditor may conduct interviews with relevant employees and management, review a representative sample of customer files and transactions, perform transaction testing, evaluate the handling of unusual activity alerts and internal reports, and assess the implementation and effectiveness of AML/CFT controls across the business.

The audit shall also evaluate the Company's implementation of corrective actions arising from previous audit findings, regulatory inspections, compliance reviews, or internal monitoring activities, including whether Senior Management and the Board have taken timely and appropriate action to address identified deficiencies.

The scope, methodology, findings, recommendations, and conclusions of each independent AML/CFT audit shall be documented in a written audit report. Any deficiencies, control weaknesses, or instances of non-compliance shall be reported to Senior Management, the Board of Directors (or equivalent governing body), the MLRO, and other relevant control functions, as appropriate.

Senior Management shall ensure that appropriate corrective actions are implemented within agreed timeframes to address all identified deficiencies. Progress against remediation plans shall be monitored until all actions have been satisfactorily completed. Where necessary, the Company shall strengthen its AML/CFT controls, policies, procedures, systems, or training programme to address identified risks and ensure continued compliance with applicable legal and regulatory requirements.

The results of the independent AML/CFT audit shall be retained in accordance with the Company's Record Retention Policy and shall be made available to the Curaçao Gaming Authority or any other competent authority upon request.

17. REGULATORY SUPERVISION AND EXAMINATION

The Company acknowledges the supervisory, inspection, and examination authority of the Curaçao Gaming Authority ("CGA") in relation to its AML/CFT/CPF obligations and shall cooperate fully with the CGA in the exercise of its regulatory functions.

The Company shall provide the CGA, upon request, with timely access to all records, information, documents, systems, personnel, and other materials necessary to enable the CGA to assess the Company's compliance with applicable AML/CFT/CPF laws, regulations, licence conditions, regulatory standards, and this Policy.

The Company shall ensure that all relevant records, customer information, transaction records, risk assessments, internal reports, audit reports, training records, and other AML/CFT/CPF documentation are maintained in a complete and accessible manner and are made available to the CGA during supervisory reviews, inspections, examinations, or investigations, subject to applicable legal requirements.

The Company shall cooperate fully with any regulatory examination, inspection, information request, or compliance review conducted by the CGA and shall promptly implement appropriate corrective actions to address any findings, recommendations, or remedial measures identified by the CGA within the prescribed timeframe.

Senior Management and the Board of Directors shall ensure that adequate resources are made available to facilitate regulatory examinations and to support the timely remediation of any deficiencies identified by the CGA.

18. REVIEW AND UPDATE

The Company shall ensure that its Anti-Money Laundering and Counter-Financing of Terrorism ("AML/CFT") policies, procedures, and controls are subject to regular review and are kept up to date to ensure their ongoing effectiveness and compliance with applicable legal and regulatory requirements.

Such reviews shall take into account, at a minimum:

- changes in applicable laws, regulations, and regulatory guidance, including requirements issued by the Financial Intelligence Analysis Unit and other competent authorities;
- changes in the Company's business model, products, services, delivery channels, customer base, and geographical exposure;
- findings arising from the Business Risk Assessment ("BRA"), Customer Risk Assessments ("CRA"), compliance monitoring activities, internal audits, and independent reviews; and
- emerging money laundering and terrorist financing ("ML/FT") risks, trends, and typologies.

The AML/CFT framework shall be subject to a **formal review at least annually**, and more frequently where material changes, deficiencies, or elevated risks are identified.

Any proposed amendments to the AML/CFT framework shall:

- be appropriately documented, including the rationale for the changes;
- be reviewed and approved by the Board of Directors or an appropriately authorised body; and
- be communicated to relevant Personnel in a timely manner.

The Company shall ensure that updated policies and procedures are effectively implemented, and that relevant Personnel receive appropriate training or guidance in respect of any material changes.

Customer Risk

Risk Indicator	Low (1)	Medium (2)	High (3)	Extreme (4)
Identity Verification	Fully verified customer with reliable documentation	Minor verification concerns resolved	Additional verification required	Identity cannot be satisfactorily verified
Occupation / Employment	Stable and verifiable employment or income source	Limited information available	Higher-risk occupation or unclear income source	Income source unverifiable or suspicious
Source of Funds	Clear and consistent with profile	Additional clarification required	Source of funds difficult to verify	Source of funds unexplained or suspicious
Source of Wealth	Reasonable and consistent with activity	Limited information available	Requires further verification	Unexplained wealth or significant inconsistencies
PEP Status	No PEP exposure	Domestic or former PEP	Foreign PEP	High-risk PEP with additional risk indicators
Adverse Media	No adverse media identified	Minor historical issues	Credible allegations of financial crime	Ongoing criminal investigations or serious allegations
Customer Behaviour	Consistent with expected profile	Minor deviations from expected activity	Significant unexplained deviations	Activity indicative of money laundering or criminal conduct

Geographical Risk

Risk Indicator	Low (1)	Medium (2)	High (3)	Extreme (4)
Country of Residence	EU/EEA or equivalent low-risk jurisdiction	Moderate-risk jurisdiction	FATF Grey List jurisdiction	FATF High-Risk, sanctioned, or prohibited jurisdiction
Nationality	Low-risk jurisdiction	Moderate-risk jurisdiction	Higher-risk jurisdiction	Sanctioned or prohibited jurisdiction
Source of Funds Jurisdictions	Low-risk jurisdiction	Moderate-risk jurisdiction	Higher-risk jurisdiction	Sanctioned or non-cooperative jurisdiction
IP Address/Geolocation	Consistent with declared residence	Occasional travel or temporary differences	Frequent use of multiple jurisdictions	Concealed or suspicious location activity
Jurisdiction Risk Exposure	No elevated risks identified	Limited higher-risk exposure	Significant exposure to higher-risk jurisdictions	Exposure to sanctioned or prohibited jurisdictions

Transaction Risk

Risk Indicator	Low (1)	Medium (2)	High (3)	Extreme (4)
Deposit Activity	Consistent with customer profile	Moderate transaction volume	High transaction volume	Excessive or unexplained transaction volume
Withdrawal Activity	Consistent with gameplay activity	Minor anomalies identified	Unusual withdrawal behaviour	Withdrawal activity indicative of ML concerns
Wagering Activity	Recreational gambling behavior	Elevated but explainable activity	High-volume gambling activity	Activity lacking apparent gambling purpose

Deposit-to-Withdrawal Ratio	Consistent with normal gambling patterns	Minor irregularities	Significant Irregularities	Rapid movement of funds with minimal gambling activity
Payment Method Usage	Single verified payment method	Multiple verified payment methods	Frequent changes to payment methods	Third-party or suspicious payment method activity
Transaction Patterns	Normal customer behaviour	Occasional monitoring alerts	Repeated unusual transaction	Structuring, layering, or suspicious transaction patterns
Trigger Events	No trigger events identified	Single trigger events	Multiple trigger events	Significant trigger events

Delivery Channel Risk

Risk Indicator	Low (1)	Medium (2)	High (3)	Extreme (4)
Onboarding Method	Remote onboarding with full KYC verification	Remote onboarding with supplementary checks	Enhanced verification required	Verification cannot be completed
Device Risk	Single known device	Multiple verified devices	Multiple unverified devices	Device activity indicative of account misuse
IP Address Risk	Consistent with customer profile	Occasional deviations	Frequent changes requiring review	VPN, proxy, TOR, or location concealment detected
Account Access Behaviour	Normal access patterns	Minor anomalies	Unusual login behaviour	Account sharing or account takeover indicators

RISK CLASSIFICATION GUIDANCE

- Low Risk customers may be subject to simplified or standard monitoring measures, where appropriate.
- Medium Risk customers shall be subject to standard Customer Due Diligence (“CDD”) and ongoing monitoring measures.
- High Risk customers shall be subject to Enhanced Due Diligence (“EDD”) and enhanced ongoing monitoring measures.
- Extreme Risk customers fall outside the Company’s standard risk appetite and shall generally not be onboarded or maintained unless exceptionally approved in accordance with the Company’s AML/CFT framework.

Any override of the calculated risk rating shall:

- be appropriately justified;
- be documented in writing; and

be approved by the MLRO or other authorised person, where applicable

ANNEX B- CRA RISK RATING METHODOLOGY

The Company applies a risk-based scoring methodology as part of the Customer Risk Assessment (“CRA”) process.

Customer risk shall be assessed across the following categories:

- Customer Risk;
- Geographical Risk;
- Product and Service Risk; and
- Delivery Channel Risk.

The operational indicators and scoring criteria applicable to each category are set out in Annex A — CRA Risk Scoring Matrix.

Indicative Risk Scoring

Risk Level	Score
Low	1
Medium	2
High	3
Extreme	4

The overall customer risk classification shall be determined based on:

- the overall assessment of relevant risk indicators;
- the combination of identified risks; and
- professional judgement.

Customers may be classified as:

- Low Risk;
- Medium Risk;
- High Risk; or
- Extreme Risk.

Any manual override of a risk classification shall be documented and appropriately approved.