

Mr. Cedric Pietersz
Curaçao Gaming Authority
Scharlooweg 172-174
Willemstad-Curaçao

30 May 2025

Re: Uploading AML/CFT Policy

Dear Mr. Pietersz,

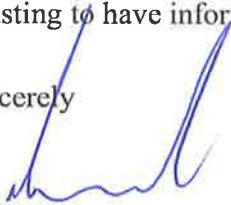
In order to comply with the due date for submission of the AML/CFT Policy, the applicant hereby uploads the draft version of the AML/CFT policy.

Note that this policy is not yet final as it is under review by management for approval and sign off.

Once approved, the final and official version will be signed off by management and uploaded to the portal. We expect this to take place in the course of the coming week.

Trusting to have informed you accordingly.

Sincerely



Raoul Behr
Managing Director

Anti-Money Laundering and Countering Financing of Terrorism Policies

BRIGHT WIN LIMITED B. V.

VERSION CONTROL

Date of Adoption	Version and Description	Approved/Reviewed by
January 30, 2024	Version 1 – Adoption of the Policy	Senior Management and External Consultants
February 18, 2025	Version 2 – Changes pursuant to audits and review	Senior Management and External Consultants
May 2025	Version	

This document is to serve as a policy handbook for managing the day-to-day affairs of the management, employees and agents pertaining to Anti Money Laundering (“**AML**”), Counter Terrorist Financing (“**CTF**”) and sanctions measures, policies and controls adopted by the Company (“**AML Policy**”). All employees, agents, and the management of the Company shall ensure the implementation of this AML Policy and detection, prevention and management of risks associated with the day-to-day affairs and business.

1. Overview

Bright Win Limited B.V. ("**Company**") has been operating on the brokerage structure for many years. However, the Company is now looking to transition into a brokerage and a B2B agency model. Under the B2B agency model, the Company will deal with direct deposits and withdrawals from customers as well as the deposits and withdrawals through distribution networks ("**Agents**"). Under the new model, the Company will sign an agreement with the B2C operating Agent who will then onboard the downline players to participate on the Company's platform, and the Company will provide the Agents with the technology and the relevant compliance and account management support. In return the Agent will get rebates from the revenue brought in by the Agents/ Players onboarded by them.

It is the Company's policy to prohibit and actively prevent money laundering and terrorist financing and any activity that facilitates such actions or any other criminal activities by complying with all applicable laws and international standards issued by international bodies such as FATF, UNSC, OFSI, GCB, UKGA etc. ("**Relevant Laws**") and monitoring the adequacy of such policies, procedures and internal controls in order to prevent and detect money laundering and terrorist financing offences. Offences under the regulatory framework governing AML and CTF can be committed by any of the customers, the Agents, the Company, its employees, depending on their respective levels of knowledge or suspicion.

This AML Policy serves as a guidance to the AML and CTF policies and procedures by raising awareness of its challenges and dangers to the Company's daily operations. The objective of this AML Policy is to educate and train the employees, Senior Management, key intermediaries, agents on our compliance requirements, policies, processes, and controls in respect of our commitments towards AML and CTF. As explained in greater detail in the subsequent sections, the offences under the regulatory framework governing AML and CTF can be committed by the Agents, the players onboarded by the Agents ("**Bettors**"), the senior management or the employees of the Company, depending on their respective levels of knowledge or suspicion. The Company's Money Laundering Reporting Officer ("**MLRO**") and the AML compliance department comprising the MLRO, Board and persons appointed by them collectively, shall be responsible for keeping this AML Policy up-to-date.

This AML Policy focuses primarily on the money laundering risks presented by the transactions with the Bettors, and other business-to-business partners, including any third parties acting on behalf of the Company. Failure to manage the ML/TF risks can expose the Company to not only statutory and regulatory non-compliance but also to reputational and financial threat, imposition of financial penalties at corporate and personal level. They can also result in action against senior management, Agents and Bettors for failing to deploy and operate an appropriate system of internal control. Failure to adhere to the provisions of this AML Policy may also subject the Agents and employees to disciplinary action including immediate termination of their engagement. The Company will report violations to the appropriate regulator or law enforcement authorities as required by the Relevant Laws.

Since the Company's business spans across multiple jurisdictions, please note that this AML Manual has been prepared keeping the best practices in mind with reference to the UK and EU AML and CTF regulatory framework. This AML Manual shall be promptly updated in due course depending on the jurisdiction where the Company receives Tier 1 license. All the employees, directors, senior management, Agents and the persons acting on behalf of the Company will familiarise themselves with this AML Policy, what may constitute a crime of ML/TF and the policies and procedures to be adhered to prevent this crime from taking place within the Company. The MLRO will regularly and at least on an annual basis review its contents with the relevant process and subject to the approval from the Board, amend as required. Furthermore, in accordance with this AML Policy, policies and procedures shall be developed that will be adhered to by all the Agents (as applicable to them), employees, senior management and persons acting on behalf of the Company to prevent opportunities for money laundering in relation to the Company and its activities.

2. Background on Money Laundering and Terrorist Financing

What is meant by Proceeds of Crime?

AML and CTF regulatory frameworks are applicable to proceeds of crime. Broadly, proceeds of crime are property from which a person benefits directly or indirectly, by being party to criminal activity. This criminal property could be stolen money, money from drug dealing or property stolen in a burglary or robbery. It could also include property which the criminal gains by spending the proceeds of criminal activity.

Money laundering in a nutshell

Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. Even passive possession of criminal property, irrespective of the amount, would qualify as a money laundering offence. It is our duty to be vigilant at all times in all aspects of our business as criminals continuously probe to find weaknesses in the system and look at various methods to launder illegally obtained money.

Where a person intentionally commits, or assists in the commission, of any criminal act (indicative list set out below) in respect of property derived from any of the offences, such person shall be considered to have committed the offence of money laundering:

- Narcotics and psychotropic substances;
- Kidnapping, piracy and terrorism;
- Offences in violation of the environmental law;
- Illicit dealing in firearms and ammunition;
- Bribery, embezzlement and misuse of public funds;
- Fraud, breach of trust and related offence;
- Corporate theft or any white-collar crimes.

Criminal property typically means monies, or any other tangible property derived from the following offences:

- Conversion, transfer or deposit of the proceeds of crime with intent to conceal or disguise their illicit origin; and
- Concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to or ownership of proceeds.

A person who commits any of the acts listed above is considered a perpetrator of the offence of ML as per the Relevant Laws. The Company itself may be criminally liable for that offence if such an activity is intentionally committed in its name or for its account. Accordingly, it becomes more imperative for the Company to ensure that the Agents onboarded and the persons acting on behalf of the Company are also in compliance with this AML Policy and the Relevant Laws.

There are three acknowledged phases to money laundering:

- Placement
- Layering
- Integration

Placement: First phase of money laundering, commonly known as 'Placement', involves infiltration of monies derived from proceeds of crime into the relevant jurisdiction's legitimate financial system. This is the point when proceeds of crime are most apparent and at risk of detection. Since banks and financial institutions are strictly mandated to develop, monitor and implement AML procedures, criminals look for other ways of placing cash within the financial system. Gambling and betting companies can be targeted because they and their practices commonly deal with deposit and usage of customer's money for betting and gambling purposes.

Layering: Once the proceeds of crime are in the financial system, layering involves obscuring the origins of the proceeds by passing them through complex transactions. These often involve different means and can take place in multiple jurisdictions. Some of the common means include:

- Anonymous customers laundering or spending the proceeds of crime
- Accessibility of multiple premises/remote operators

- False or stolen identity documentation used to bypass controls.

Integration: Once the origin of the funds has been obscured, the criminal is able to make the funds appear to be legitimate funds or assets. A customer may deposit funds and then not use the player account for a significant period of time before looking to withdraw the funds at a later stage, following very little or no activity, in the hope to distance themselves from crimes by the passing of time. This is the most difficult stage at which to detect money laundering.

There is potential for the money launderer to use gambling at every stage of the process. The instances of using cash transactions, identity theft and identity fraud can enable the money launderer to move criminal proceeds with anonymity. Furthermore, the use of multiple internet transactions can facilitate the layering stage of money laundering. The applicable AML and CTF measures further include detection of criminal lifestyle spend. There are also implications for the Company to consider where the crimes included in the definition of a predicate offence differ across jurisdictions, for example tax evasion.

Money laundering is relatively unique, insofar as court proceedings can be brought without predicate offences that result in subsequent money laundering activity.

What is Terrorist Financing?

What is Financing of the Proliferation of Weapons?

Proliferation Financing (PF) refers to the provision of funds or financial services used to facilitate the manufacture, acquisition, and movement of nuclear, chemical, or biological weapons and their delivery systems. In line with the Curaçao Gaming Control Board Regulations, the Company has incorporated risk-based controls to detect and prevent PF risks and will treat PF with the same scrutiny as ML and TF.

CTF is a further area to consider because terrorists and their supporters may commit crimes in order to finance acts of terrorism. Although the intended destination and usage of funds is different from money laundering, the behaviours and methods in which the funds are moved through the system are very similar. The Company should therefore be aware that the practical implementation of risk mitigation measures for terrorism financing and money laundering activity, will involve the monitoring of very similar activities and behaviours, which are set out in greater detail in the remaining sections of this AML Policy.

Terrorist financing typically involves solicitation, collection or provision of funds with the intention that they may be used to support a terrorist act or organization. The mainstream methods to raise funds used by terrorist organizations include:

- Private donations by terrorist supports / sympathizers
 - Abuse and misuse of non-profit organizations and charities
 - Criminal activity
 - Legitimate commercial activity

Terrorist financing often involves a complex series of transactions; like money laundering, this generally follows three separate phases:

- Collection: funds are often acquired through seeking donations, carrying out criminal acts, or diverting funds from genuine charities.
- Transmission: where funds are pooled and transferred to a terrorist or terrorist group
- Use: where the funds are used to finance terrorist acts, training, materials, accommodation, and propaganda, etc.

However, like the three-stage model of money laundering, this model is fairly simplistic, so it is important not to get caught up in trying to determine if an activity follows this pattern. Instead, the Company must focus on whether there is knowledge, suspicion, or reasonable grounds for knowledge or suspicion. The Company shall ensure that its employees and Agents are vigilant in following the process set out in this AML Policy, in this regard.

3. Regulatory Framework and the Company's Obligations

In addition to the international standards referenced, the Company explicitly adheres to all applicable Curaçao laws and regulations, including:

- National Ordinance on the Reporting of Unusual Transactions (NORUT), last updated June 2024;
- National Ordinance on Identification of Customers when Rendering Services (NOIS), last updated June 2024;
- Sanctions National Ordinance and the Kingdom Sanction Law
- Curaçao Financial Intelligence Unit (FIU) guidance
- Curaçao Gaming Control Board Regulations (January 2025 update).

These obligations take precedence where conflicts arise with international guidance.

Being a business involving acceptance and withdrawal of money, the Relevant Laws require us to play our part in the international effort to combat the threats of money laundering and terrorist financing by deploying appropriate measures to identify and anticipate such activities.

While the Company is incorporated in Curacao and regulated under license thereunder, it aims to comply with international best practices and more specifically the regulations set in Tier 1 jurisdictions such as the UK and the recommendations issued by FATF and other international bodies like the OFAC, OFSI, OECD etc. Therefore, it is imperative to ensure that effective risk assessments, policies, procedures and controls are in place to prevent ML/TF and continue to raise standards in that regard.

The Company has carefully considered the following Relevant Laws which shall act as the guiding principles in the adoption and implementation of this AML Policy:

- Recommendations issued by the Financial Action Task Force (FATF)
- The UK Proceeds of Crime Act, 2002
- The UK Terrorism Act, 2000
- The UK Gambling Act, 2005
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, 2017
- Fourth and Fifth Money Laundering Directives issued by the European Union
- General recommendations from the UNSC on AML and CTF compliance measures
- Laws applicable in countries where the Company carries out its business.

The AML Policy, procedures, systems and controls thereunder make appropriate use of any relevant findings, recommendations, guidance, directives, resolutions, sanctions, notices, or other conclusions, that may be published from time to time. Furthermore, the FATF typology reports assist the Company in identifying new money laundering and terrorism financing threats. The Company is further required to ensure that the following elements of an AML and CTF framework are in place:

- Streamline Agent and Player KYC & AML checks at onboarding to drive a competitive experience with automated risk screening and through media searches as well.
- Designate MLRO at the management level. The MLRO shall be appointed by the Senior Management of the Company and shall have requisite experience in laws, industry best standards, policies and procedure pertaining to KYC, AML and CTF compliances.
- Establish internal controls, communication, and reporting procedures, which will include the customer due diligence and Agent on-boarding policy, ongoing monitoring of relationships and transactions with customers, Agents etc.
- Monitor the relevant economic thresholds set out in this AML Policy and flag the risks to Senior Management and/ or the MLRO (as the case maybe) in the event such thresholds are breached and/or the customers/Agents/customers of the Agents/transactions are classified as high-risk categories in order to ensure the Company remains in full compliance of this AML Policy.
- Establish guidance and procedures for identifying and reporting suspicious / irregular activities to the MLRO.
- Establish procedures for carrying out Customer Due Diligence ("CDD") for the determination and verification of the true identity of the customers of the Company and the Agents and their source of funds, prior to establishing the relationship. For the purposes of validating the source of funds, the Company shall obtain certified copies of the bank statements of the end customers or proof of business (business registration/ incorporation certificate) in case of Agents.
- Institute appropriate procedures for awareness and training of employees, agents and persons acting on behalf of the Company on the implementation of this AML Policy and effective monitoring of the procedures and controls established by the Company in accordance with this AML Policy to

ensure that Company's business is conducted in compliance with the Relevant Laws.

- Checks carried out in real time to ensure compliance across multiple time zones, whatever the time of day. Identify worrying gaming patterns, like early withdrawals with our transaction monitoring solution adapted for responsible gaming

The Relevant Laws in respect of AML and CTF measures are usually applicable to proceeds of crime. Broadly, proceeds of crime is defined to mean any property from which a person benefits directly or indirectly, by being party to criminal activity. This criminal property could be stolen money, money from drug dealing or property stolen in a burglary or robbery. It could also include property which the criminal gains by spending the proceeds of criminal activity. For instance, a player onboarded by an Agent spending money gained in a wrongful manner like theft, fraud etc. to place bets with the Agent.

Sanctions and penalties

The Company must comply with Curaçao-specific sanctions laws, including direct implementation of UN, EU, and Kingdom Sanctions as required by the Kingdom Sanction Law. Upon identification of a sanctioned individual or entity, funds must be immediately frozen, and a report filed with the FIU Curaçao.

The Company must comply with any sanctions, embargos or restrictions in respect of any person or state to which the UN, UK, FATF or EU has decided to apply such measures ("**Sanctions**"). The Company shall and the MLRO shall ensure that the Company conducts sufficient due diligence on the Bettors to ensure that it does not: (a) act for any Sanctioned persons or entities, and (b) violate any of the Sanctions. All measures to identify persons or entities covered by sanctions will be documented. The Company shall comply with the Sanction regime set out below:

<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>

https://assets.publishing.service.gov.uk/media/675301707e5323915d6a0409/Counter-Terrorism_Domestic_.pdf

The Company shall comply with guidance issued by OFSI on 'reporting information to OFSI – what to do', which is relevant for external accountants, auditors and tax advisers.

<https://www.gov.uk/guidance/suspected-breach-of-financial-sanctions-what-to-do>

The Company shall use the background screening software, Refinitiv World Check One ("**Screening Software**") to run the player entries (names, birth year and place) against Sanction lists, legal and regulatory directions, law enforcement lists, negative news, adverse media, local and international government records, PEPs. The Company shall not onboard/ continue business relationship with any person who is identified to be a Sanctioned person or a person acting on behalf of any Sanctioned person/entities or a PEP and their engagement shall be immediately terminated. If any Bettor or third party engaged with the Company breaches any of these sanctions, embargos or restrictions or is found to be in these sanctions list, it will report these to the relevant authority in accordance with this AML Policy.

To ensure compliance with applicable regulatory framework and mitigate risks associated with sanctions, Politically Exposed Persons (PEPs), and negative media, the Company shall follow the below mentioned screening procedures for Bettors and Agents:

Initial Screening

- The Company utilizes the Screening Software, to screen all new Agent names at the time of onboarding and all Bettors when they hit the thresholds of deposits or losses in excess of XCG 4000 in accordance with CDD requirements set out in this AML Policy ("CDD Threshold").
- Screening shall, at all times, include checks against sanction lists, PEP lists, law enforcement lists, negative news, adverse media, and local and international government records covered within the Screening Software.
- For Agents, the screening shall extend to their Ultimate Beneficial Owners (UBOs), directors, and other controlling individuals, where applicable.
- In the event of unresolved matches and hits against the screened individuals, the Compliance Team shall prepare a report setting out findings regarding the accuracy of the matches. In the event the matches do not accurately relate to the screened individual, the account relationship shall be continued and in cases of true matches the account relationship shall be immediately terminated.
- The Company is required to conduct ongoing screening for all accounts, including bettors and agents, to account for the dynamic nature of sanctions, adverse media, and PEP connections.
- Periodical screenings shall be conducted at a minimum frequency of half yearly for all accounts, and quarterly checks on accounts flagged as medium risk.
- A detailed Background Screening Policy adopted by the Company for all the Agents and direct customers is attached to this AML Manual as Annexure IV.

Employee Responsibilities

- Employees conducting Customer Due Diligence (CDD) are responsible for ensuring that all customer screening obligations are adhered to in accordance with the Background Screening Policy set out to the AML Manual as Annexure IV. This includes:
 - Ensuring that all data is correctly inputted into the screening system.
 - Escalating any flagged accounts to the MLRO for further investigation.
 - Documenting all screening results and maintaining records in compliance with this AML Policy.

Governance and Reporting

The results of screenings and updates to flagged accounts shall be reviewed by the MLRO and in escalation cases, Senior Management. Actions taken in response to flagged results shall be documented for regulatory compliance.

Risks Associated with Dealing with Sanctioned Persons, Countries, or Corporate Entities

Engaging in business with sanctioned persons, countries, or corporate entities poses significant legal, financial, and reputational risks to the Company. Sanctions are imposed by international bodies such as the United Nations (UN), European Union (EU), Financial Action Task Force (FATF), or national governments (e.g., UK Office of Financial Sanctions Implementation - OFSI) to combat activities like money laundering, terrorist financing, and other forms of organized crime. Breaching sanctions may result in severe penalties, including substantial fines, restrictions on operations, loss of business licenses, and criminal liability for the Company and its management. Furthermore, such breaches can lead to reputational harm, loss of stakeholder trust, and increased scrutiny from regulatory bodies. It is essential to ensure that the Company's operations, including those carried out by its agents, customers, and

partners, are fully compliant with all applicable sanctions regimes. Proactive screening and due diligence are crucial to mitigate these risks and uphold the Company's commitment to ethical and lawful business practices.

Disciplinary action against employees

Employees are required by their terms of employment to comply with the matters set out in this AML Policy, including their personal obligation to participate in AML awareness training and to make an internal Suspicious Activity Report ("**SAR**") to the MLRO if they know or suspect or have reasonable grounds for knowing or suspecting that a person may be engaged in money laundering or terrorist financing. Failure to do so may lead to disciplinary action, up to and including dismissal.

4. Senior Management

Senior management of the Company shall comprise the heads of different functions of the Company's business, namely, Compliance, Operations, Finance, Technology and Marketing. Senior management must be fully engaged in the processes of the Company's assessment of risks for money laundering and terrorist financing, and must be involved at every level of the decision making to develop the Company's policies and processes to comply with the Relevant Laws. The Senior management shall specifically take responsibility and exercise due skill, care and diligence for the following:

- 4.1. Compliance with this AML Policy and the policy, procedures and controls put in place thereunder.
- 4.2. Adopting a risk-based approach to AML, establishing and maintaining effective policies, procedures, systems and controls to prevent opportunities for money laundering in relation to the Company and its business activities.
- 4.3. Ensure that the Company's systems and controls include provision to provide senior management/ the board with regular management information on the operation and effectiveness of its AML systems & controls necessary to identify, measure, manage and control the Company's money laundering risks.
- 4.4. Ensure that AML Policy and the procedures, systems and controls established thereunder enable the Company to:
 - determine whether a Bettor or a beneficial owner is a Politically Exposed Person ("**PEP**").
 - comply with the Relevant Laws.
- 4.5. Carry out regular risk assessments of the adequacy of the Company's AML and CTF systems and controls to ensure that they continue to enable it in identifying, assessing, monitoring and managing money laundering risks adequately.
- 4.6. Ensure that an appropriate person is appointed as the MLRO, at all times, to undertake roles and responsibilities set out for the MLRO in this AML Policy.
- 4.7. Ensure that employees are adequately trained and comply with the relevant requirements of the Company's AML Policy and the procedures, systems and controls established thereunder.

5. Money Laundering Reporting Officer (MLRO)

The Relevant Laws require the Company to develop the appropriate compliance management arrangements and appoint a designated MLRO to ensure strict adherence with the AML Policy and the procedures, systems and controls established thereunder.

Pursuant to a decision made by the Senior Management, the Company has appointed Mr. John Lavado. The MLRO shall be supervised by an expert agency or individual who shall act as the external MLRO (collectively with the internal MLRO, referred to as the "**MLRO**") in a supervisory capacity to head and supervise the AML, CTF and Legal compliance team of the Company. Pursuant to a decision made by the Senior Management, the Company has appointed an external MLRO. The employees shall report to the MLRO on any AML and CTF related discussions, disclosures and matters, as specified in greater detail in the remaining sections of this AML Policy.

The MLRO's contact details are set out below:

Email Address: mlro@brightwinlimited.com

The MLRO will have direct access to the Director and CEO and shall be responsible to ensure compliance with this AML Policy, the related procedures and controls and the Relevant Laws. The designated MLRO, shall have a minimum of 7 years of experience in AML, compliance, or legal functions within the real money gaming/ gambling or financial services or similar industry, preferably with relevant certifications in AML, KYC, or financial crime compliance. The MLRO's primary role includes overseeing the firm's AML/CTF framework, developing and implementing AML policies, conducting risk assessments, monitoring transactions, undertaking or assisting in regulatory audits and ensuring timely reporting to regulatory authorities. Additionally, the MLRO shall facilitate employee training and maintain an ongoing dialogue with Senior Management to uphold a strong compliance culture within the Company.

The MLRO's responsibilities shall specifically include:

- 5.1. Ensuring that the Company is in compliance with the Relevant Laws;
- 5.2. Ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;
- 5.3. Advising and training Senior Management, employees and persons acting on behalf of the Company in developing and implementing internal policies, procedures and controls in accordance with this AML Policy;
- 5.4. Promoting compliance with the Company's AML Policy and taking overall charge of all AML/CTF matters within the Company;
- 5.5. Carrying out the day-to-day operations for compliance with the Company's AML Policy;
- 5.6. Acting as the point of contact to receive information and coordinate requests from the employees and the Agents regarding AML and CTF issues;
- 5.7. Submitting External Suspicious Activity Report ("SAR") to the relevant authority and/or the Senior Management (as the case maybe), following the AML compliance check, if the players' or Agents' funds are known or suspected to have criminal origins; In the Curacao legislation unusual transaction reporting is required. Where in this manual Suspicious Activity Report ("SAR") are mentioned; unusual transaction reporting is applicable.
- 5.8. Establishing SAR procedures and arranging for the maintenance of electronic copies of all underlying documentation;
- 5.9. Acting as the point of contact within the Company for relevant authorities;
- 5.10. Promptly informing the Senior Management and the relevant departments of the Company if the Company receives a request for information from a regulator or agency responsible for AML or CTF or Sanctions breaches;
- 5.11. Reviewing any relevant government, regulatory and international findings, recommendations, guidance, directives, resolutions, Sanctions, notices or other conclusions pertaining to AML or CTF;
- 5.12. Assisting in establishing, developing and coordinating the Company's monitoring procedures for AML purposes;
- 5.13. Taking reasonable steps to establish and maintain an appropriate AML and CTF training program and adequate arrangements in accordance with this AML Policy for staff, as well as the Agents and persons acting behalf of the Company;
- 5.14. Identifying appropriate instances to perform enhanced due diligence on potential clients;
- 5.15. Within 30 days from the end of each quarter, reporting to the CEO, Board of Directors and the Compliance Committee on the results of the review of AML Policy, AML & CTF Measures, Risk Assessment Matrix and AML Training conducted during the quarter.

- 5.16. Annually reviewing the effectiveness of the AML & CTF measures adopted by the Company and presenting a report on the findings of such review to the CEO and the Board highlighting the measures that can be adopted to address any adverse findings
- 5.17. Coordinating the review and response to AML audit(s).

6. Customer Due Diligence Policy

CDD Thresholds and Timelines:

Under NOIS and NORUT, the CDD threshold is NAF. 4,000 (or equivalent). Once a customer meets or exceeds this threshold, compliant documentation must be collected within 30 days. If not received, the account must be suspended or terminated, and a report may be submitted to the FIU.

6.1. Risk based Approach:

As per the Relevant Laws and industry best practices, the Company has adopted effective risk assessments, policies, procedures and controls to detect and prevent money laundering and terrorist financing and to keep crimes and proceeds of crimes out of the Company's business. The latest version of the Company's Risk Assessment Matrix is attached to this AML Policy as **Annexure I ("RA Matrix")** which must be followed by all employees, Agents and persons acting on behalf of the Company to ensure effective compliance with the Relevant Laws and this AML Policy. The RA Matrix adopts an approach which is proportionate to the risk exposure of the Bettor. These risks will be evaluated in the context of the nature of its business, players, structure of the business, jurisdictions, products, services, payment modes and any other matters which are relevant in the context of money laundering risks associated with the Company's business. The effectiveness of the RA Matrix shall be reviewed and assessed annually, and the RA Matrix (as reviewed annually) should outline key risks along with consequences, mitigating controls, risk ratings and owners.

The risk-based approach involves taking discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the Company. These steps require us to undertake the following steps, which are described in greater detail in RA Matrix:

- Risk Identification: identify and analyse the money laundering and terrorist financing risks that are relevant to the Company's business.
- Risk Mitigation: design and implement appropriate policies, procedures and controls to effectively manage and mitigate the identified and assessed risks.
- Risk Monitoring: monitor and improve the effective operation of these policies, procedures and controls to reflect any change in operator risk profile.
- Documentation: record internal controls in the form of policies and procedures to ensure that staff are able to carry out their AML obligations.
- Risk-review: Evaluating the application of controls and procedures to ensure that policies are fit for purpose.

The MLRO and the Senior Management shall regularly monitor and, on an annual basis, review the RA Matrix adopted by the Company. Any changes to the same, shall need to be approved by the Senior Management and adopted in this AML Policy in **Annexure I**.

- 6.2. Identifying Risks: The Company will undertake a risk-based assessment of Bettors, and assign them a risk rating proportional to the money laundering risk posed. The objective of assigning a risk rating is to determine the course of action to be adopted with the Bettor and level of diligence to be carried out. The detailed parameters for categorizing the risk posed by the customers is set out in the RA Matrix. Format of the Risk Assessment Form is set out in **Annexure II**.

While conducting a risk assessment the following shall be taken into consideration:

- Identify the Bettor and any beneficial owner(s) pursuant to the documents required for completing CDD in the manner set out in this AML Policy;

- Take into consideration the Bettor's country of origin, residence, nationality, and place of incorporation or place of business (if corporate);
- Obtain information on the purpose and intended nature of the business relationship;
- Where a corporate entity is involved, take into consideration the nature of the Agent, its ownership and control structure, and its beneficial ownership (if any), including its possible status as a PEP.
- Carry out background checks using third party service providers/internal systems in case of suspicious activity or upon EDD Thresholds set out in this AML Policy being met;
- Take into consideration the relevant product, service or transaction with the Company.

When relying on sources other than documents, the Company must ensure that the methods (which may include checking references with other financial institutions and obtaining financial statements) and sources of information are appropriate, and in accordance with Company's policies and procedures and risk profile of the Bettor. A brief snapshot of risk identification (which has been set out in greater detail in the RA Matrix) is set out below for the ease of reference and understanding:

Low Risk Accounts

Low risk accounts shall require the Company to undertake CDD at the time these accounts cross the CDD Threshold in this AML Policy. These accounts will be monitored annually for any updates to the risk rating.

Medium Risk Accounts

Based on the CDD process and background verification, country of origin, nature and location of activity, and the customer profile, the accounts that may pose a higher-than-average risk in accordance with the RA Matrix, may be classified as medium risk.

This category of accounts will be monitored quarterly and may also be changed to high risk due to lack of information or doubt on accuracy or if some information comes to the knowledge of the Company which increases the risk associated with the account.

High Risk and Very High Risk Account

Based on the following parameters, the Company may determine an Agent or a Player to be a high-risk account:

- Suspicious activities, lack of information or the accuracy thereof and the business relationship being conducted in unusual circumstances;
- Businesses and sources of wealth that are cash-intensive;
- Complex and unusual ownership structures involving trusts, private investment vehicles etc.
- Accounts opened or operated from high-risk jurisdictions not having adequate AML & CTF regime;
- Sanctions lists, entities and countries as identified by publicly available data, credible sources or Screening Software and PEPs with significant levels of criminal activity;
- Payment received from a third party and not from the account holder themselves.

The Company shall not deal with/ onboard/ operate high risk and very high-risk accounts, without the approval of the MLRO and the Senior Management.

Governments in many countries have enacted legislation to make money laundering and terrorist financing criminal offences and have legal and regulatory processes in place to enable those engaged in these activities to be identified and prosecuted. Internationally, FATF has done a great deal to encourage governments to adopt minimum standards including, making their

national regulators require financial services firms in their jurisdictions to follow specific due diligence procedures in relation to Players and the Agents in high-risk jurisdictions.

Where higher risk countries such as Iran, Cuba, and North Korea are identified, the MLRO must be notified immediately for guidance on what additional procedures may be necessary and on how to proceed. UNSC Sanctions and sanctions issued by other international or government bodies may apply to a number of jurisdictions, bodies or individuals. Sanctions change regularly and as such, if in any doubt, contact the MLRO immediately before proceeding further. The Company, its employees and the Agents shall also make use of the Screening Software to obtain risk scores and screen players and the Agents against the Sanctions List.

The employees, the Agents and persons acting on behalf of the Company shall strictly comply with the CDD requirements set out in this AML Policy. All individuals opening an account must be over the age of 18, which shall be validated in case of Agents prior to the account opening and in case of Players upon such players crossing the CDD Threshold. Allowing persons below the age of 18 to bet on its platform is an offence under various Relevant Laws and the minimum compliance standards.

Age of the Bettors shall be verified through proof of ID and other supporting documents like passport copies, government identification certificates etc. In the event the Company has a reasonable apprehension to believe that a Better has been in violation of this requirement, the account with such Bettor shall be immediately terminated.

The Agents within the agency structure are bound by the same obligations as set out in this AML Policy in respect of CDD and KYC requirements, which includes age verification prior to account opening and onboarding of a Bettor. Furthermore, the Agents shall provide the Company with a quarterly report setting out the player P&L position of each player onboarded by them on the cut-off date ("**P&L Report**"). If a player meets the transactional threshold set out in the AML Policy, based on P&L Report, the Compliance Team shall immediately trigger enhanced due diligence. At this point, the Agent will provide all source of wealth documentation and details of the player for further examination by the Company.

6.3. **Customer Due Diligence Requirements:**

Agents: The Company shall perform CDD on Agents prior to establishing business relations or conducting any transactions with the Agents. The Company shall obtain from the Agents, information pertaining to their identity as set out in detail below and such information shall be documented for record keeping purposes. The Agents onboarded by the Company shall also comply with the obligations of conducting and satisfy themselves of CDD and KYC of the Player prior to their onboarding. These controls shall be tested by the Company on a quarterly basis. In case of failure by an Agent to comply with this requirement detailed further in this AML Policy within the timelines stipulated therein, the Agent's account and its business relation with the Company shall be terminated in accordance with the terms of this AML Policy.

Direct Customers: The Company shall perform CDD on all the direct customers who hit the CDD Threshold or when Company has doubts about the accuracy and completeness of any information requested/ obtained or in the event of an account change in the risk categorisation of the account into a medium risk account due to suspicious activity being identified.

6.4. **Documents Verification**

Based on the knowledge and understanding obtained during the interactions with potential customers, and the Agents, Company shall establish the following:

- In case of individuals (being either a Player or an Agent), the Company shall require the following:
 - ✓ Full name of the customer
 - ✓ Unique identification number (Passport, Govt-issued photo ID, etc.)
 - ✓ Proof of address along with the proof thereof

Proof of Address must:

- Be detailing the customer's name and residential address;
- Match the details provided by the customer to the Company;
- Be a utility bill dated within the last 3 months or government issued identity card referencing the addressing which requires government verification at the time of obtaining.

✓ Nationality

✓ Date of birth

- For verification of the identity of the Agents registered as an entity, the Company shall require the following:

✓ Full business name of entity

✓ Business Incorporation or registration number

✓ Existing registered and mailing business address

✓ Contact details of the authorized representatives

✓ Date and place of incorporation and certificates evidencing the same

✓ Charter documents and the AML policies and procedures adopted by the Agent, if any

✓ Information from UBO, Directors and Partners with shares more than 10% of the entity, which includes:

- Full Name, Address, Date of Birth, and Nationality
- Government Issued ID (Proof of Identity - POI)
- **Certified** Proof of Address (POA)
- Source of Wealth information
- A certified confirmation adhering to the 10% UBO threshold
- When appropriate, company structure charts
- A **register of shareholders** of the corporate Agent
- A **register of directors** of the corporate Agent
- POI and POA of each director of the corporate Agent, as per the CDD guidelines set out in this Section for CDD on individuals
- **Identification of the Ultimate Beneficial Owner (UBO)**—defined as any natural person owning at least 25% of the share capital of the corporate Agent—and obtain:
 - (a) POI and POA of such UBO as per the CDD guidelines set out in this Section for CDD on individuals, and
 - (b) Source of Wealth documentation to ascertain the origin of the UBO's wealth

In case of the documents collected from individuals (being the Players or individual traders as Agents and the UBOs/Directors/Partners of the corporate Agents) as a part of the CDD:

- The Government issued identity card (being either a passport or any other government issued national identity proof) must (“**POI**”):
 - ✓ Be a clean copy detailing the holder’s name, date of birth, place of issuance, issuing country or a governmental department of the Company, validity, issuance and expiry date (if any), include a clear photograph of the Customer;
 - ✓ Match details provided by the Bettor to the Company.
- The proof of address must (“**POA**”):
 - ✓ Detail the Agent or the Player’s name and physical residential address;
 - ✓ Match the details provided by the Agent or the Player to the Company.

In case of the documents collected from Agents as a part of the CDD, following factors must be considered when verifying the documentation:

- Has all required documentation been supplied for all Directors, Signed Signatories and Power of Attorney’s;
- Does the application signature match that of one of the directors;
- Do the Agent’s Articles of Association confirm the Directors of the Company as per the declared details on the application and the signed signatory list;
- Do signatories’ or powers of attorney holder’s signatures match against passports supplied;
- Does the board resolution signature match against the signature of one of the signatories;
- Registered corporate name and any trading name matches against the trade license and registration documents exactly and as detailed on the application;
- Does the Agent’s website (if any) confirm relevant information given on the application and compares against the documents supplied.

Furthermore, in case of Agents being corporate entities, in addition to the above, the Company shall obtain the following documents from such corporate Agents:

- A register of shareholders of such corporate Agent
- A register of directors of such corporate Agent
- POI and POA of each director of such corporate Agent as per the CDD guidelines set out in this Section for CDD on individuals
- Documents to identify the Ultimate Beneficial Owner (i.e. person owning at least **25%** of the share capital of such corporate agent, down to a natural person) (“**UBO**”) and obtain (a) the POI and POA documentation of such UBO as per the CDD guidelines set out in this Section for CDD on individuals, and (b) source of wealth documentation of such UBO to ascertain the source of such UBO’s wealth.

- 6.5. Ongoing and Enhanced Due Diligence (“**EDD**”): Customers should be continually monitored by the relevant employees of the Company and the Agents for any update in their risk profile. Where behaviors or transactions are identified which may increase the customer’s potential risk, further investigations and due diligence should be undertaken. Factors which may increase a customer’s risk, may include the triggering of an internal or suspicious activity, EDD Thresholds set out above being met, a match against a PEP/Sanctions list or a sudden change in behavior, such as increase in depositing frequency and/or amount.

The Company shall conduct EDD verifications and checks in the following cases (“**EDD Thresholds**”):

- In case of Bettors with gross settlements of XCG 5.000 within a rolling 365 days period and obtaining the relevant diligence documents for validating source of wealth in such cases, in accordance with the terms of this AML Policy.
- There is a suspicion of money laundering or terrorist financing in any of the Bettor accounts onboarded that exhibit suspicious activity as defined by the MLRO, in alignment with the minimum Compliance Standards.
- In the event of a change in the risk categorisation of the Bettor account into a medium risk account due to suspicious activity being identified.
- In case the Company/Agent has doubts about the accuracy and completeness of any information previously obtained.

The internal transaction monitoring systems shall be used by the Company for monitoring transactions by the bettors within 15 days from the end of each quarter. On a designated date each month, the Compliance Team shall extract and review a report identifying all Bettors who have exceeded the Enhanced Due Diligence (EDD) thresholds as stipulated under this Policy. For each such Bettor, the Company shall require the submission of appropriate Source of Wealth (SOW) documentation. Operators and their onboarded Agents shall likewise be responsible for monitoring their respective downline players against the EDD thresholds and shall promptly notify the MLRO and Senior Management upon the identification of any such occurrence. EDD should follow the risk-based principle, in that where the customer’s ML risk increases so should the level of due diligence performed on the customer. The aim of EDD is to obtain a level of confidence that the account is not funded by the proceeds of crime or used to finance terrorism.

Therefore, in the event, the Company’s employees or Agents or persons acting on its behalf: (a) reasonably believe suspicious activity/ behavior linked to an account, (b) are dealing with high-risk customers, and when EDD Thresholds are met, EDD shall be carried by them to ensure due compliance with this AML Policy. In such cases, the Compliance department shall, obtain certified copies of documents pertaining to such account holder’s source of funds in the manner set out in this AML Policy. The EDD of such account holders shall be validated by the MLRO and the Senior Management before approving the account, till which time such accounts shall remain suspended.

There are various processes detailed below which shall be used by the Company to mitigate the ML or TF concern associated with the transactions between the Company and the Bettors who have met the EDD Thresholds:

- Third-party verification: use of approved third parties to conduct verification of customer documents.
- Validation of customer documents: Certified copies of documents establishing source of wealth of the Bettors. For the purposes of validating the source of wealth, the Company and/or the Agents (as the case maybe) shall obtain certified copies of the bank statements of the account holder or proof of business (business registration/ incorporation certificate), net worth certificate certified by lawyers/ chartered accounts/ regulatory bodies, property documents, salary certificates etc. Corroborate sustainable wealth that matches the customer’s gambling profile. This may also overlap with responsible gambling considerations. Accurately identifying a customer’s source of funds and source of wealth can be a complex process and one in which approaching an online customer directly for relevant evidence may be a last resort.
- Background and lifestyle checks: Using open-source research to obtain further information about the Bettor’s source of wealth, occupation, property ownership status and lifestyle.
- Internal corroboration of user identity: This could emanate from a variety of sources from customer monitoring, other databases and third-party verification where possible.

Acceptable documentation for identification of Source of Wealth determination for users who hit the EDD thresholds shall include the following:

- Salary/ Employment Income: Pay slips (last 6 months), employer confirmation letter, Income Tax returns, bank statements (showing salary deposits).
- Business Ownership: Audited financial statements, company registration and valuation reports, tax returns, bank statements (business income deposits).
- Investments: Shareholding certificates, dividends reports, portfolio statements, investment deeds.
- Inheritance: Will/ probate documents, bank statements showing fund transfers.
- Real Estate: Property sale agreement, rental income statements, land registry documents.
- Other Legitimate Sources: Any documentary evidence supporting funds, with explanation from the customers. Documents must be recent (issued within the last 6 months). The MLRO may request additional documentation where required. Third-party verification may be conducted through open-source data and public records.

Risk Assessment and Documentation of Justification: For all customers meeting the EDD threshold set out herein:

- An internal risk assessment report will be generated by compliance officers to substantiate how the customer's documented wealth justifies their betting activity.
- This will include a narrative/rationale document, explaining:
 - Wealth sufficiency: Does the documented income / wealth reasonably support the gambling activity?
 - Percentage of declared wealth used: If gambling expenditure exceeds 50% of declared wealth, additional scrutiny is required.

The MLRO will review and Senior Management shall be required to approve such requests before account continuation in all such cases.

6.6. Politically Exposed Person: A PEP is an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors and high-ranking officers in armed forces;
- members of the administrative, management or supervisory bodies of state-owned enterprises;
- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents.

- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the Bettor into a higher risk category. A foreign PEP presents a higher risk of money laundering because there is a greater risk that such person, if he was committing money laundering, would attempt to place his money offshore where the Agent or the player is less likely to be recognized as a PEP and where it would be more difficult for law enforcement agencies in his home jurisdiction to confiscate or freeze his criminal property.

As a part of the Company's policy, it will ensure that it does not enter into relationships with individuals where it is known, or the Company and/ or the Agent has substantial reasons to believe that funds are derived from corruption or misuse of public assets. The Company, its employees and the Agents shall make use of the Screening Software to obtain risk scores of a customer on the basis of their historical play and transactions are used to help identify suspicious activity by the customers.

The decision to open an account for a PEP should be taken by the Board and the CEO in discussion with the MLRO. The CEO in consultation with the MLRO shall identify the Bettor, record the reasons for onboarding such Bettor and make special arrangements to address the risks associated with such Bettor to ensure that the Company does not unknowingly assist in hiding or moving the proceeds of corruption by PEPs, their families or associates.

PEP accounts will be subject to more rigorous documentary and other due diligence requirements. Adequate measures will be taken by the relevant employees of the Company and the Agents to cater to the higher risk factors:

- Analysis of any complex structures, for example involving trusts or multiple jurisdictions;
- Development of a profile of expected activity for the business relationship in order to provide a basis for transaction and account monitoring;
- Initial screening and due diligence prior to the account opening;
- Ongoing and periodical screening of accounts opened by PEPs;
- Detailed KYC;
- Purpose and use of the account;
- Location of the accountholder(s);
- Employment / earning history;
- Checking source of wealth, type of transactions to be conducted through the account, and jurisdictions involved in such transactions;
- Probing the account holder's employment or business history; and
- Scrutinizing the account holder's sources of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and reviewing monies coming from government, government controlled, or government enterprise accounts (beyond salary amounts).

The Company shall treat individuals as PEPs for at least 12 months after they cease to hold a prominent public function. However, family members and known close associates of PEPs are treated as ordinary clients from the time that the PEP ceases to discharge a prominent public function.

7. Compliance Obligations and Training

7.1. Employee Obligations and Liabilities:

The Company's compliance with the AML Policy and internal procedures and controls put in place under the AML Policy is the responsibility of each employee, Agent and any other individual who acts on its behalf.

Each employee, Agent and any other individual who acts on its behalf will:

- Comply with the requirements set forth in this AML Policy and other relevant policies and procedures of the Company in this regard, particularly those related to client identification and verification.
- Make reasonable efforts to determine the true identity of the Agents and the Players.
- Develop and maintain a clear understanding of their practices, and report activities identified as unusual/suspicious to the MLRO.

In case of the Agents, these obligations shall be more specifically set out in the Agent agreement which shall be entered into between the Company and the Agent prior to Agent onboarding going live. Each Agent shall be: (a) provided with the training materials and the Company's AML Policy, and (b) duly informed by the Company on the AML Policy and procedures of the Company along with the minimum compliance standards.

7.2. Outsourcing of the Obligations

In the event that the Company outsources any of the processes/requirements under this AML Policy viz. the CDD and EDD requirements, to any third-party service provider, it will ensure compliance with, and be liable for any failure to meet such requirements/ obligations. The Company shall undertake adequate diligence and care to satisfy itself of the credibility/ suitability of the third service provider to discharge such services. Any decision to outsource any obligation under this AML Policy or to rely on the third-party service provider to outsource shall need the approval of the Senior Management and the Board of Directors of the Company.

7.3. Employee Training:

One of the most important controls for the prevention and detection of money laundering is to have employees, Agents and persons acting on behalf of the Company who are alert to the risks of money laundering and terrorist financing, and who are well trained in the identification of unusual activities or transactions which appear to be suspicious, as well as in the accurate verification of customers' identities.

The effective application of even the best designed control systems can be quickly compromised if the persons implementing and applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the Company's AML and CTF strategy.

Therefore, all the employees and persons acting on behalf of the Company shall be trained to:

- Understand the Relevant Laws, AML Policy, Risk Assessment Matrix, data protection policy and other relevant policies, procedures and control established thereunder ("**AML & CTF Measures**").
- Apply the AML & CTF Measures in day-to-day operations of the Company.
- Report suspicious activities to the MLRO.

The Company shall have the following obligations in this regard and the MLRO along with the Senior Management shall ensure that the Company is in compliance with them:

- Ensure that the employees and persons acting on behalf of the Company are made aware of the Relevant Law, the requirements of data protection, and the AML & CTF Measures adopted by the Company, at the time of their onboarding process.

- Conduct annual AML and CTF training where the employees and persons acting on behalf of the Company are given training on the AML & CTF Measures adopted by the Company and how to apply them in day-to-day operations to recognize and deal with transactions or activities or situations which may be related to money laundering or terrorist financing ("**AML Training**").
- Maintain a record in writing and monitor the effectiveness of the AML Training to ensure that all employees are trained in an appropriate and timely manner, and that the training is fit for purpose.
- In addition to the AML Training, ongoing training must be given to all relevant employees at appropriate intervals. Records should be maintained to monitor who has been trained, when they received the training, the nature of the training and the effectiveness of the training.

7.4. **Agent Training:**

In addition to the training of the employees in the manner set out above, the Company shall and the Senior Management shall ensure that the Company provides adequate AML and CTF training to the Agents at the time of onboarding and on a half yearly basis, thereafter to help the Agents in: (a) understanding and managing AML risk better, (b) complying with their obligations/requirements under this AML Policy, including CDD, EDD, reporting, documentation obligations etc., and (c) applying the AML & CTF Measures in the day to day operations pertaining to the business relationship with the Company.

The MLRO and the Senior Management shall be responsible for devising and managing the delivery of such training, taking particular care to ensure that systems are in place to cover all Agents (the super masters, masters and agents) and employees (part- time or casual).

The training related information set out above shall be brought to the attention of new employees and Agents and will remain available to all employees and Agents via the Company's internal systems (through intranet or such other appropriate modes, as maybe adopted by the Company from time to time).

8. **Identifying and Reporting Suspicious Transactions**

- 8.1. **Suspicious Transactions:** The Company shall monitor on an ongoing basis, its business relations with every customer, and Agent including transactions as well as any other material change in each customer's/Agents' identification information. The Company shall further, during the course of business relations, observe the conduct of the customer's/Agents' account and scrutinise transactions undertaken to ensure that the transactions are consistent with the Company's/agents' knowledge of the customer, and where appropriate, the source of funds.
- 8.2. The employees, Agents and persons acting on behalf of the Company shall be obliged to make a report in respect of information that comes to them in the course of their day-to-day operations:
 - where they know;
 - where they suspect;
 - where they have reasonable grounds for knowing or suspecting;

that a person is engaged in money laundering or terrorist financing, including criminal spend, or attempting to launder money or finance terrorism. In this AML Policy, these obligations are collectively referred to as 'Grounds for Knowledge or Suspicion'.

In order to provide a framework within which suspicion reports may be raised and considered, the MLRO must consider each such report, and determine whether it gives grounds for knowledge or suspicion. If the MLRO determines that a report does give rise to grounds for knowledge or suspicion that a person, whether or not a customer, is engaged in money laundering, the MLRO must report the matter to the designated regulatory authority under the Relevant Laws.

Suspicious activity shall specifically include the following:

- Transactions which have no apparent purpose and make no obvious economic sense, or which are designed or structured to avoid detection;
- An Investigation concludes that there is evidence of money laundering or terrorist financing which is deemed by the MLRO to be indicative of attempted money- laundering;
- Insufficient or inaccurate documentation/ information (EDD or Source of Wealth etc.) provided when requested to substantiate the level of activity, which is deemed by the MLRO to give rise to suspicion regarding the provenance of funds as also an example in line with the Mandatory Compliance Standard;
- Transactions requested by a Person without reasonable explanation, which are outside the ordinary range of services normally requested or are outside the experience of the Company in relation to the particular Bettor, or deliberately structured to avoid detection;
- Where, without reasonable explanation, the size or pattern of transactions is out of line with any pattern that have previously emerged;
- The Bettor refuses to provide information requested without reasonable explanation;
- Where a Bettor uses the business relationship for a single transaction or for only a very short period of time;
- An extensive use of offshore accounts, companies or structures in circumstances where the party's needs do not support such requirements;
- Unnecessary routing of funds through third party accounts;
- Unusual transactions without an apparently profitable motive;
- Payments involving cash;
- Payments from illegal, suspicious, non-related to business sources, personal or business checks drawn on non-related, suspicious, Company/personal bank account, and third-party checks where there is no clear connection of the third party to the underlying transaction;
- Money fund passing activity wherein two or more colluding parties intentionally transfer funds from one account to the other, where the sole purpose and motive is to transfer funds in contradiction to the platform's purpose and make it appear legitimate (i.e. gambling winnings).
- Any other suspicious activity as set out by the MLRO.

The Curacao legislation is based on unusual transaction reporting and objective and subjective reporting requirements. The unusual transactions based on a objective must be reported by the MLRO within 48 hours to the FIU.

- 8.3. Internal reporting: The first level of reporting of suspicious activities and the grounds for knowledge or suspicion of money laundering and terrorist financing, is by the employees, Agents and the persons acting on behalf of the Company to the MLRO on the designated email of the MLRO as set out in this AML Policy ("**Internal Report**"). The Internal Report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the grounds for knowledge or suspicion of money laundering or terrorist financing. The Internal Report should be documented or electronically recorded, in the manner set out in greater detail in **Annexure III**. All internal enquiries made in relation to the Internal Report should also be documented or electronically recorded. This information may be required to supplement the initial Internal Report or as evidence of good practice and best endeavours if, at some future date, there is an investigation by a law enforcement agency.

- 8.4. Evaluation by the MLRO and External Reporting: The MLRO must consider each report and determine whether it gives rise to grounds for knowledge or suspicion of money laundering and terrorist financing. Unusual transactions based on an objective indicator must be reported within 48 hours to the FIU. Unusual transactions based on a subjective indicator must be reported to the FIU within 48 hours after it was concluded the transaction is unusual.

The MLRO may also require further information to be obtained from the customer and/or the agent (as the case maybe), if necessary. Any approach to the customer and/or the agent (as the case maybe) should be made sensitively and preferably by someone already known to the customer and/or the agent (as the case maybe), to minimise the risk of alerting the customer and/or the agent and/or an intermediary (as the case maybe) that a disclosure to the regulatory agencies is being considered. If the MLRO decides not to make a report to the regulatory authorities, the reasons for not doing so should be clearly documented or electronically recorded and retained. The MLRO must make a disclosure to the regulatory authorities where the MLRO decides that an Internal Report gives rise to grounds for knowledge or suspicion. The known or suspected money laundering activity must be reported to the FIU or the equivalent regulatory body responsible for implementing the AML and CTF policies of the relevant jurisdiction in which the transaction, which is known or suspected to involve money laundering, is located.

- 8.5. Failing to report: Failing to report information giving rise to the knowledge or suspicion of suspicious activity under the AML regulatory framework is a criminal offence, which can lead to prosecution and potential liabilities to the Company, the MLRO and the employees / persons acting on its behalf. The Senior Management and Board of Directors, shall: (a) ensure that Internal
- 8.6. Reporting and Exporting is carried out by the designated responsible persons in accordance with this AML Policy. Additionally, regular quarterly updates are obtained from the MLRO, covering Internal and External Reporting. These updates detail key AML and CTF concerns, governance issues, any identified suspicious or unusual activity, and operational challenges encountered during the quarter. This comprehensive reporting framework ensures thorough oversight and continuous improvement in our compliance and risk management processes.
- 8.7. Tipping off, or prejudicing an investigation: Under the Relevant Laws, any employee, Agent or persons acting on behalf of the Company shall be deemed to have committed an offence of tipping off, if they:
- The disclosure is likely to prejudice any investigation that might be conducted following the disclosure referred to above.
 - The information on which the disclosure is based came to the person, in the course of the Company's business.
 - The information on which the disclosure is based came to the person, in the course of the Company's business.
 - Make a disclosure which is likely to prejudice the investigation.
 - Falsify, conceal, destroy or otherwise dispose of, or cause or permit the falsification, concealment, destruction or disposal of documents which are relevant to the investigation.

The Relevant Laws, in this regard, contain separate offences of tipping off and prejudicing an investigation. These offences are similar and overlapping, but there are also significant differences between them. There are a number of disclosures which are permitted and that do not give rise to these offences.

Once an Internal or External Reporting has been made, it is a criminal offence for anyone to release information that is likely to prejudice an investigation that might be conducted following that disclosure. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice an investigation, or if the disclosure is permitted under the Relevant Laws.

9. Obligations of the Company's Agents

The Company's Agents and their employees are subject to the Relevant Laws, policies and procedures, designed to combat money laundering and terrorist financing activities, within their respective countries. This AML Policy shall act as a reference for identification, record keeping and reporting requirements for transactions, specific to the Agent's jurisdiction. This AML Policy shall be shared by the Agents with their employees and persons acting on their behalf. The Agents may choose to implement additional internal requirements keeping in mind the best practices of their business, so long as such requirements are not inconsistent with those given in this AML Policy and by the Relevant Laws.

Prior to onboarding of an Agent which is an entity, the Agent shall, and the Company through the MLRO shall ensure that the Agent. It is hereby clarified that in case of individual Agents, the individuals themselves shall be considered for compliance with the Agent's obligations under this AML Policy:

- Designates a qualified person responsible for the implementation of this AML Policy and other relevant policies, procedures and control established thereunder ("**Compliance Officer**"). The Compliance Officer shall be trained by the Company in the manner that the employees are trained on the implementation of this AML Policy and AML & CTF Measures by the Agent.
- Provides the Company with a declaration in writing confirming that the said Agent and its Compliance Officer have reviewed the AML Policy and AML & CTF Measures adopted by the Company and received relevant training regarding the same.

The Compliance Officer shall be the person responsible for AML and CTF compliance by the Agent in respect of the transactions carried out by the Agent on behalf of the Company. The responsibilities of the Compliance Officer shall specifically, include:

- Overseeing and monitoring adherence by the agent to this AML Policy and policies and procedures established thereunder.
- Ensuring training of the Agent's employees at the relevant levels to ensure adherence to this AML Policy.
- Reporting and ensuring that the Agent and its employees identify and report suspicious activity to the MLRO in the manner set out in this AML Policy and identification requirements.
- Ensuring that all employees of the Agent at relevant levels, review periodic AML and CTF compliance training and educational materials provided periodically by the Company to the Agent.
- Providing supplemental training to employees of the Agent as needed to address compliance deficiencies with the AML Policy that are noted through monitoring, regulatory audits or program adherence reviews.
- Ensuring that the initial and ongoing training is documented and maintained and retained in accordance with local record keeping requirements.
- Reviewing all suspicious activity reporting by the Agent's employees for accuracy, completeness and timely submission to the MLRO.
- Developing and implementing appropriate corrective action for any deficiencies identified during the monitoring process.
- Ensuring that employees follow the AML compliance processes as set out in this AML Policy at all times when engaging in the transactions on behalf of the Company.
- Monitoring transaction activity using daily reports, investigating any significant deviations from normal trends, where applicable.

- Ensuring that all documents relating to consumer transactions are retained in a safe and secure place in compliance with local regulations and this AML Policy.
- Serving as the primary contact with the Company's AML compliance team, senior management and MLRO. In addition, when needed, serving as a contact during regulatory audits by the Company.

Sanctions, PEP and Adverse Media Checks

Prior to establishing a business relationship with an Agent, the Company shall in the event, (i) Agent is a corporate entity, the Company shall run screening checks against the Agent as well as the names of the Ultimate Beneficial Owner (UBO) and the Directors of such Agent(s), and (ii) Agent is an individual, the Company shall run screening checks against such individual Agent.

The Company shall use the background Screening Software to run the Agents and UBO entries, as well as Players onboarded by Agents who hit the CDD thresholds against Sanction lists, legal and regulatory directions, law enforcement lists, negative news, adverse media, local and international government records, etc. in respect of Sanctioned persons/entities. The Company shall not onboard/ continue business relationship with any person who is identified to be a Sanctioned person or entity or a person acting on behalf of any Sanctioned person/entities and their engagement shall be immediately terminated.

The Company shall have the right to conduct surprise checks and audits to ensure compliance by the Agent of this requirement, without the requirement of notifying the Agent. The Company shall be conducting periodical sample tests to ensure that the Agents are following this requirement in the manner envisaged in the Policy. The Background Screening Policy adopted by the Company for all the Agents and direct customers is attached to this AML Manual as **Annexure IV**.

Suspicious Activity Reporting

In case of any suspicious activity identified by the Agent in accordance with Section 8 above, the Agents shall prepare and share an Internal Report with the Company and MLRO, in the manner set out in greater detail in Section 8 read with Annexure II. The Internal Report should be documented or electronically recorded. The Internal Report should include full details of the player who is the subject of concern and as full a statement as possible of the information giving rise to the grounds for knowledge or suspicion of money laundering or terrorist financing.

Regulatory Inquiries

From time to time, the Company may receive requests from regulatory bodies and law enforcement agencies. If the Agent's employees receive such a request, they must report it to the MLRO as soon as practicable.

Agent Record keeping

Agents and their employees must obtain and record all consumer information required by the Company in accordance with this AML Policy and the Relevant Laws. All such information obtained by the Agents must be retained along with all forms, receipts, reports and any supporting documentation.

Employees of the Agent conducting transactions on behalf of the Company must obtain and record all information required by identification and record keeping policies and procedures. Employees must ensure that all required information is contained in the customer details and suspicious activity reporting forms.

10. Authorized Payment Channels

Cash presents an inherent risk of money laundering due to difficulties with traceability. The ability to identify and verify the source of funds, and the activities which generated those funds, is a requirement under the Relevant Laws and directives that apply to the Company. Cash transactions pose significant obstacles to the Company in meeting these requirements. Cash is recognised by FATF as a key money laundering vulnerability.

Accordingly, the Company shall and the Senior Management shall ensure that any fund settlements between the Company and the Agents are made from authorised banking channels/licensed payment service providers in the name of the recipient and there shall be no third party funding and no cash receipts accepted for payments receivable by the Company. The Company shall ensure that all its direct customers open a designated account with licensed PSPs where the Company maintains an account (currently, Jeton and ASPAC) and provide the Company with the details of the accounts maintained by them with such licensed PSPs in the form of the Payment Services Agreement or account opening letters or account statements. Customers shall deposit funds upfront with the Company using the licensed PSP pursuant to which equivalent credit shall be assigned to the customer. Thereafter, amounts shall be settled between the Company and the customers on a monthly basis using the said licensed PSPs.

11. Termination of business relationship with the Bettors

To avoid potentially committing one of the principal money laundering offences, the Company needs to consider ending the business relationship with a customer in the following circumstances:

In case of a Player:

- where it is known that the customer is attempting to use the Company, its Agents or persons acting on its behalf to launder criminal proceeds or for criminal spend.
- where the risk of breaches the Relevant Laws are considered by the Company to be too high.
- where the customer is identified as a Sanctioned person or a person acting on behalf of Sanction persons/entities.
- where the customer's gambling activity leads to an increasing level of suspicion, or actual knowledge of, money laundering.
- where the customer is proven to a reasonable degree of confidence to not be the identity they claim to be.

Additionally, where, in relation to any customer, the Company is unable to apply CDD and EDD measures or if the customers fail to furnish information/ documents requested by the Company, the business relationship with the customer *must* be terminated after a period 28 days from the date such measures/ requirements are triggered.

In case of an Agent:

- where it is known that the Agent is attempting to use the Company or persons acting on its behalf to launder criminal proceeds or for criminal spend.
- where the risk of breaches the Relevant Laws are considered by the Company to be too high.
- where the Agent is identified as a Sanctioned person or a person acting on behalf of a sanctioned person.
- where the Agent's transactions lead to an increasing level of suspicion, or actual knowledge of, money laundering.
- where the Company finds the Agent to be in breach of the requirements set out in Section 10 above and such breach remains uncured by Agent for a period of 28 days from the date of such breach.
- Where the Agent and/ or the Compliance Officer appointed by it fail to provide the Company with:

- ✓ information that it may require regarding any player / transaction in case of an inquiry or investigation within 28 days of the Company requisitioning such information from the Agent by way of a written notice.
- ✓ information pertaining to EDD on players and transactions undertaken by the Agent or upon such player accounts meeting the transactional thresholds set out in this AML Policy, within 14 days of such thresholds being met.

12. Reporting & Recording

The MLRO will report to the Company's senior management on a Quarterly basis, on the following matters:

- The Company's compliance with its requirements under the Relevant Laws;
- The quality of the Company's AML & CTF Measures and any suggestions for improvements and modifications;

The results of the review of AML & CTF Measures and AML Training and any national or international findings and how the Company will take these findings into account;

- Any Internal Reporting made by the Company's employees and the action taken in respect of those reports, including the grounds for all decisions;
- Any External Reporting made by the MLRO and the action taken in respect of those reports, including the grounds for all decisions; and
- Any of the relevant matters related to money laundering as it concerns the Company's business.

The Company's senior management will promptly take action, as required subsequent to the quarterly AML Compliance update, in order to resolve any identified deficiencies.

The Company shall make and keep records set out in this AML Policy (viz. KYC, Reporting documents etc.) and these records shall be safely kept with the Company for a minimum of ten (10) years. All records shall be kept in line with the Relevant Laws. In circumstances where a criminal investigation is being undertaken all records will be kept until the Authorities advise otherwise.

13. Annual Review

Within 30 days from the end of each financial year, the MLRO shall complete the annual review of AML Policy, AML & CTF Measures, RA Matrix and AML Training & Awareness programs and provide the Board of Directors, the CEO and the Senior Management with the Annual AML & CTF Compliance Report ("**Annual Compliance Report**"). The Annual Compliance Report will examine the effectiveness of the AML & CTF measures adopted by the Company against the data collected from the operations. In the Annual Compliance Report, the MLRO shall highlight the suggested mitigants for the issues raised, including any amendments/ changes to the AML Policy, RA Matrix and AML Training & Awareness programs to ensure that the Company's AML & CTF Measures are effective and robust in detection of money laundering and/ or terrorist financing.

The Senior Management shall review the Annual Compliance Report and undertake necessary actions to update the AML Policy and procedures to remedy the concerns highlighted therein.

Operator Review

For Agents and B2C Operators, the Company shall conduct independent audits on all downline operators on a quarterly basis, with a minimum interval of three months (3) months between audits, to assess ongoing compliance and operational integrity in accordance with the framework set out in **Annexure V** of this AML Manual.

The Operator shall be evaluated against standards through the application of a Risk Threshold Framework. Each compliance category or control area, will be assessed to determine the adequacy and effectiveness of the controls in place. The outcomes of this assessment shall be documented in a Compliance Action Plan, which will detail any required remedial actions and timelines for implementation.

The scoring methodology shall be based on the RA Matrix (BRAM), which applies a defined risk impact framework to evaluate each compliance category. This assessment will determine the sufficiency and effectiveness of existing compliance controls. A Risk Identification Matrix shall be employed to classify the findings, and the resulting analysis will inform subsequent discussions regarding the formulation and implementation of appropriate remedial actions.

Upon identification of compliance deficiencies, a Compliance Action Plan shall be developed to prescribe the necessary corrective actions along with associated implementation timelines. Identified risks shall be classified according to the following severity levels:

- **High Risk** – Remedial action required within seven (7) calendar days
- **Medium Risk** – Remedial action required within fourteen (14) calendar days
- **Low Risk** – Remedial action required within thirty (30) to sixty (60) calendar days

For each assessed compliance criterion, the Compliance Action Plan will detail the specific deficiency, the corrective measure required, and the recommended timeframe for resolution.

Failure to implement the prescribed corrective actions within the stipulated timelines—inclusive of a thirty (30) day grace period during which follow-ups will be conducted - may result in the suspension or termination of the Operator's account.

Additionally, an external review shall be undertaken by external auditors within 30 days at the end of each fiscal year to independently assess and validate the Company's implementation and effectiveness of its Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) compliance framework, including all relevant processes and internal controls.

14. ANNEXURE I

BUSINESS RISK ASSESSMENT MATRIX

[To be attached separately]

15. ANNEXURE II

AML RISK ASSESSMENT FORM

This should be completed at the beginning of the transaction, during the transaction if anything changes and just before the transaction is completed. Assessment of risk should take both client and transaction risk into consideration and will dictate whether Standard or Enhanced Client Due Diligence (CDD) is required.

INITIAL ASSESSMENT OF RISK:	LOW (Standard CDD)	MEDIUM (Standard CDD)	HIGH (Enhanced CDD)
Please note below reasons for your assessment:			
SIGNED BY:	DATE:		

INTERIM RISK ASSESSMENT – HAVE ANY RISK FACTORS CHANGED?	LOW (Standard CDD)	MEDIUM (Standard CDD)	HIGH (Enhanced CDD)
Please note below reasons for your assessment: <i>(If no, quick note stating as such, signed and dated – evidences that a review has been undertaken and consideration has been made)</i>			
SIGNED BY:	DATE:		

FINAL RISK ASSESSMENT – HAVE THERE BEEN ANY LAST- MINUTE CHANGES THAT GIVE CAUSE FOR CONCERN?	LOW (Standard CDD)	MEDIUM (Standard CDD)	HIGH (Enhanced CDD)
Please note below reasons for your assessment: <i>(Should be undertaken before monies are transacted/enter the client A/C)</i>			
SIGNED BY:	DATE:		

If you have assessed the risk as high at any point during the transaction or have any reservations or concerns, please refer to the MLRO before continuing to act for the client.

16. ANNEXURE III

SAR – INTERNAL REPORTING FORMAT

Details of the Customer:

- Full Name:
- Date of Birth:
- Identification Document and Number:
- Postal Address:

Explanation/ description of suspicious activity(ies).

This section of the Internal Reporting is critical. The care with which it is completed by the employees or the agents may determine whether or not the described activity and its possible criminal nature are clearly understood by the MLRO. Provide a clear, complete and chronological description of the activity, including what is unusual, irregular, or suspicious about the transaction(s), using the checklist below as a guide as you prepare your account.

Suspicious Activity Information

- Describe the conduct that raised suspicion.
- Explain whether the transaction(s) was completed or only attempted.
- Describe supporting documentation and retain such documentation for your file for ten years.
- Explain who benefited, financially or otherwise, from the transaction(s), how much and how (if known).
- Describe and retain any admission or explanation of the transaction(s) provided by the subject(s), witness(s), or other person(s). Indicate to whom and when it was given. Include witness or another person ID.
- Describe and retain any evidence of cover-up or evidence of an attempt to deceive regulatory bodies, or others.
- Indicate where and at what instance the possible violation of law(s) took place.
- Indicate whether the suspicious activity is an isolated incident or relates to another transaction.
- Indicate whether there is any related litigation. If so, specify the name of the litigation and the court where the action is pending.
- Recommend any further investigation that might assist the MLRO and/ or the law enforcement authorities.
- Indicate whether any information has been excluded from this report; if so, state reasons.

- Indicate whether any foreign currency and/or foreign negotiable instrument(s) were involved. If foreign, provide the amount, name of currency, and country of origin.
- Indicate any additional account number(s), and any domestic or foreign bank(s) account numbers which may be involved.
- Indicate for a foreign national any available information on subject's passport(s), visa(s), and/or identification card(s). Include date, country, city of issue, issuing authority, and nationality.
- Describe any suspicious activities that involve transfer of funds to or from a foreign country, or any exchanges of a foreign currency. Identify the currency, country, sources and destinations of funds.
- Describe the subject only if you do not have the identifying information of the customer or if multiple individuals use the same identification. Use descriptors such as male, female, age, etc.
- Indicate any wire transfer in or out identifier numbers, including the transfer company's name.

17. ANNEXURE IV BACKGROUND SCREENING POLICY

1. Purpose

This Screening Policy (the “**Policy**”) supplements and aligns with the AML Manual of Bright Win Limited B.V. (the “**Company**”). It establishes standardized procedures for the screening of sanctions, Politically Exposed Persons (PEPs), and adverse media, both at the point of Customer Due Diligence (CDD) and on an ongoing basis. The Policy ensures compliance with applicable laws, regulatory obligations, and industry best practices.

2. Scope

This Policy applies to all Downline Operators, Agents, direct customers, players onboarded by Agents, counterparties, and beneficial owners (“**Screening Subjects**”) seeking to establish or maintain a relationship with the Company. It also extends to any third-party intermediaries, representatives, or stakeholders subject to CDD requirements under the Company’s AML framework. Screening shall be conducted at the time CDD is triggered pursuant to the AML Manual, and as part of the Company’s ongoing monitoring obligations.

3. Definitions

- **Sanctions Lists:** Consolidated databases issued by governmental or supranational authorities (e.g., OFAC, UN, EU, HM Treasury) identifying individuals, entities, or jurisdictions subject to financial restrictions or asset freezes.
- **PEP (Politically Exposed Person):** An individual entrusted with prominent public functions, including heads of state, senior government officials, judicial or military leaders, senior executives of state-owned entities, and high-ranking political party officials. The definition extends to close family members and known close associates.
- **Adverse Media/Negative News:** Publicly available information from credible sources indicating potential involvement in criminal activities, regulatory violations, corruption, terrorism, or other reputational risks.
- **Ongoing Screening:** Continuous monitoring and periodic rescreening of Screening Subjects to identify emerging risks and changes in status.

4. Roles and Responsibilities

- **Compliance Department:** Responsible for policy implementation, configuration and oversight of screening tools, adjudication of alerts, escalation of potential matches, and maintaining appropriate records.
- **Business Units / Onboarding Teams:** Must ensure that:
 - Agent accounts are not activated until screening is completed in accordance with this Policy.
 - Direct customers and Player accounts are screened upon exceeding the CDD threshold (i.e., more than XCG 4,000 within a 30-day rolling period) or upon identification of a suspicious activity or such account being classified as a higher than low risk accounts (“**CDD Threshold**”).

- **Third-Party Screening Provider:** The Company uses LSEG Risk Intelligence (Formerly Refinitiv World Check) ("**Screening Software**") to run the player entries against 1000+ sanction lists, legal and regulatory directions, law enforcement lists, negative news, adverse media, local and international government records, PEPs. The Screening Software has one of the world's largest data sets for sanctions, PEP scans and adverse media / negative news checks.

5. Screening Procedures

1. **Timing:** Screening must occur prior to account activation in case of Agents. Players must be screened upon breaching the CDD Threshold in Section 4 above.
2. **Coverage:** All Agents (individual or corporate), their UBOs, and key directors, as well as Players (upon such Players breaching the applicable CDD threshold) must be screened for:
 - Sanctions (OFAC, UN, EU, HM Treasury, etc.)
 - PEP status
 - Adverse Media / negative news

The Screening Software covers all of these in a comprehensive manner.

3. Matching Criteria:

- High-confidence true matches (exact name, DOB, or close match) require immediate escalation to the MLRO.
 - Partial or fuzzy matches are reviewed by Compliance to determine validity.
4. **Record-Keeping:** All screening results are documented in the Company Compliance google drive, referencing date of search, outcome, and responsible reviewer.

6. Ongoing Screening

1. **Ongoing Screening Feature:** While screening a Screening Subject, the Compliance Team shall select the Ongoing Screening feature available in LSEG Screening Software. On a monthly basis on an appointed date of each month, Compliance Team will undertake a review of screened Bettors to identify change in status/notifications (if any) to a positive match for sanctions or PEP classifications for previously screened Screening Subjects to see if there was any change in status as per the Ongoing Screening features which updates the results on daily basis.
2. **Frequency:** All accounts must be rescreened at least quarterly or as warranted by risk level.
3. **Event-Driven:** If changes occur (e.g., new beneficial owners, updated personal details, external intelligence on negative news), immediate screening is required.
4. **Monitoring Tool:** The Company will use automated quarterly batch screening to detect newly added sanctions or negative news.
5. **Escalation and Decision:** The following guidelines are to be applied to ensure that negative screening is done correctly.

Minimum data required: Photo identification with the following details – Full Name, Gender, Date of Birth, Nationality and Proof of Address.

Screening Risk Matrix and Follow-up Procedures

No.	Screening Results	Risk	Follow-up
1	No results returned by screening tool	Low	Pass
2	Result Returned - Identical names	Medium	Check for matching DOB and Nationality
2a	Scenario 2 + No matching DOB and No matching Nationality	Low	Pass
2b	Scenario 2 + Matching DOB and No matching Nationality	Medium	Refer to MLRO
2c	Scenario 2 + Matching Nationality and no matching DOB	Medium	Refer to MLRO
2d	Scenario 2 + Matching Nationality and Matching DOB	High	Refer to MLRO

Positive Matches:

- **Sanctions:** Immediate MLRO escalation is required. Account may be frozen and reported to relevant authority as required.
 - **PEP:** Enhanced Due Diligence (EDD) to be applied, including source of wealth verification and senior management approval. Where necessary, limit or restrict account functionality.
 - **Adverse Media:** Conduct a risk assessment. If severe or credible allegations exist, consider enhanced monitoring or account termination.
6. **Documentation:** All escalations, investigations, and decisions are recorded in the compliance case management system.

7. Training and Awareness

All relevant personnel must undergo mandatory training on screening procedures, alert handling, and regulatory expectations. Refresher sessions will be held annually or upon significant changes to applicable laws or systems.

8. Review and Updates

This Policy shall be reviewed at least annually or upon any material regulatory developments. Revisions are subject to senior management or Board approval prior to adoption.

9. Record-Keeping

All screening logs, alerts, and decisions are retained for a minimum of five (5) years or longer where mandated by applicable laws. Records must be readily accessible for internal or external audit purposes.

10. Non-Compliance and Disciplinary Measures

- Failure to follow this Policy may result in disciplinary actions, including termination of employment or engagement.
 - The Company may also be required to file suspicious transaction reports or face regulatory penalties in cases of wilful or negligent non-compliance.

ANNEXURE V

18. AGENT / B2C OPERATOR AUDIT FRAMEWORK

Introduction

This Agent Audit Process forms an integral part of Bright Win Limited BV AML Manual. It ensures that Agents and Downline Operators (“**Operators**”) remain aligned with the Company’s risk-based approach and adhere to minimum compliance standards set out herein. The process supplements the quarterly AML training, threshold based CDD and EDD reviews, and internal audits described in the AML Manual.

Purpose

The purpose of this policy is to establish a formalized and systematic process for conducting quarterly compliance audit and reviews of Operators. These reviews ensure alignment with the Company’s AML framework, regulatory obligations, and internal risk standards. The process enables identification, assessment, and mitigation of risks related to high-value transactions, suspicious activity, and customer due diligence deficiencies.

Scope

This Policy applies to all Operators, counterparties, and beneficial owners maintaining a relationship with the Company. It includes evaluation of Operator-level controls, such as:

- Player CDD & EDD documentation
- Age verification logs
- Source of Funds (SoF) validation
- SAR reporting logs and AML training records

Roles and Responsibilities

Money Laundering Reporting Officer (MLRO): Oversees policy execution, screening tools, alert adjudication, escalation management, and maintains audit records.

B2C Operators/ Onboarding Teams: Provide structured player data quarterly in the approved template.

Third-Party Screening Provider: The Company uses LSEG Risk Intelligence (formerly Refinitiv World Check) for screening names against 1000+ global lists including PEPs, sanctions, and adverse media.

Review Process

To mitigate risks associated with sanctions, PEPs, and negative media, the Company conducts quarterly reviews of players hitting CDD or EDD thresholds.

Data Requisition

Within 10 days from the end of each Quarter, all Operators must submit a data extract listing all players who meet any of the following:

- A list of all players who, within the relevant period:
 - Have recorded gross settlements of £2,000 within any rolling 30-day period;
 - Have recorded gross settlements of £100,000 within any rolling 365-day period; or
 - Have been the subject of a Suspicious Activity Report (SAR) filed during the quarter.
- A list of all identified Politically Exposed Persons (PEPs), including those detected through ongoing monitoring or screening activities conducted within the quarter.

- A list of all new Super Master Agents onboarded during the quarter, including the date of onboarding and relevant CDD status (e.g., onboarding complete, pending SoW, etc.).

Upon data validation, the MLRO/Compliance Team will select:

- 20% of EDD-threshold player records
- 10% of CDD-threshold player records

Review and Testing

Each sampled file will be tested against the following as per the controls and processes laid down in the AML Manual:

Completion of Customer Due Diligence (CDD), including verification of Proof of Identity (POI), Proof of Address (POA), and age verification requirements

Screening results covering sanctions, Politically Exposed Persons (PEPs), and adverse media, as outlined in the AML Manual

Validated and documented Source of Wealth (SoW) information

Timely and accurate risk categorization and profiling of the customer

Escalation logs for Suspicious Activity Reports, where applicable

Records of AML training provided to agents, including agent oversight and monitoring activities

Agent Onboarding controls and adherence to initial CDD requirements

PEP controls specific to agent-level screening and escalation

Controls relating to agent fund handling, reconciliation, and transparency

Evidence of Management Information Reporting framework implementation, including periodic compliance reporting and performance monitoring

Compliance Scoring

Each reviewed file is rated as:

-  Compliant – Fully meets requirements
-  Partially Compliant – Minor deficiencies
-  Non-Compliant – Material deficiencies

Remediation timelines:

- High Risk → 7 calendar days
- Medium Risk → 14 calendar days
- Low Risk → 30–60 calendar days

Reporting & Documentation:

The MLRO/ Compliance Team will produce a quarterly report that includes (“**Quarterly Audit Report**”):

- Total records reviewed
- Observations, trends, deficiencies
- Actions and remediation deadlines

Each Quarterly Audit Report shall be presented to and signed off by the Board/ Senior Management of the Company.

All reports, samples, checklists, and supporting documents will be archived in the Quarterly Operator Compliance Report Folder, in line with the Company’s 10-year recordkeeping standard.

SCHEDULE A – Sample Compliance Checklist

The following checklist shall be used when reviewing each player record sampled as part of the quarterly operator compliance review:

Review Area	Criteria	Status (✓/X/NA)
Proof of Identity (POI)	Government-issued ID verified and valid	
Proof of Address (POA)	Document issued within last 3 months	
Date of Birth	Matches ID and confirms age ≥ 18	
Sanctions & PEP Check	Screened via Refinitiv, no positive matches	
Source of Funds	Documented, credible, certified	
EDD Threshold	Trigger verified, documents collected timely	
SAR Reporting	Internal report filed if suspicious behavior noted	
Agent AML Training	Operator confirms Agent has been trained	

19. SCHEDULE B – SAMPLE TRACKER SUMMARY TEMPLATE

A summary of all reviewed files shall be logged as below:

Player Username	Agent Name	Threshold Triggered	CDD/EDD Review Status	Compliance Score ( /  / )	Remediation Due Date
--------------------	------------	------------------------	--------------------------	--	-------------------------