

Anti-Money Laundering and Countering Financing of Terrorism Policy

GET ZAPPED GAMING NV

VERSION CONTROL AND POLICY REVIEW HISTORY

Date of Adoption	Version and Description	Approved/Reviewed by
March 1, 2024	Version 1 – Adoption of the Policy	Board

This Anti-Money Laundering and Countering Financing of Terrorism Policy ("**AML Policy**") has been adopted by the Company to act as governing rules and guidance material for the staff, employees and the Senior Management to help them in effective detection, prevention and management of Money Laundering ("**ML**") and Terrorist Financing ("**TF**") risks associated with the day-to-day affairs and business of Get Zapped Gaming NV ("**Company**").

Confidentiality & Copyright - This Policy is confidential and shall remain the sole intellectual property of Get Zapped Gaming NV for the exclusive use of the employees, senior management and intermediaries of Get Zapped Gaming NV and its contents are strictly confidential and should not be copied or distributed to third parties. Get Zapped Gaming NV does not and shall not accept any responsibility or liability for any loss or damage suffered by any person arising out of the unauthorized use of, or reliance upon, this document.

1. INTRODUCTION

The rise of online gaming has brought with it a wealth of opportunities not only for players and operators, but also for crime. The Company being an egaming operator deals with direct deposits and withdrawals from customers. It is the Company's policy to prohibit and actively prevent ML and TF and any activity that facilitates ML/TF or criminal activities by complying with all applicable laws which require the Company and its employees to establish, implement and actively monitor adequate policies, procedures and internal controls in order to prevent and detect money laundering offences ("**Relevant Laws**"). This AML Policy is to serve as a guidance to the Anti-Money Laundering ("**AML**") and Combating Terrorist Financing ("**CTF**") policies and procedures adopted by the Company, in this regard.

As explained in greater detail in the subsequent sections, the offences under the regulatory framework governing AML and CTF can be committed by both the customer, the Company and its employees, depending on their respective levels of knowledge or suspicion. The Company's Money Laundering Reporting and MLRO ("**MLRO**") shall be responsible for keeping this AML Policy up-to date.

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 of the Company 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 Company's employees to disciplinary action including immediate termination of employment without payment. The Company will report violations to the appropriate regulator or law enforcement authorities as required by the Relevant Laws.

This AML Policy has been prepared keeping in mind the Company's commitment to comply with the Relevant Laws, international best practices, rules and guidance and all applicable regulations, circulars and guidelines issued by the relevant authorities. This AML Policy shall be reviewed annually and any changes to this AML Policy shall be approved by Board of Directors of the Company ("**Board**") and procedures shall be developed that will be adhered by all the 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.

All the employees, director, senior management 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. It is the responsibility of the MLRO to ensure that this AML Policy is maintained and up to date. 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.

The Company is committed to taking all reasonable measures to comply with the Relevant Laws, industry best requirements of legislation and appropriate guidelines in line with applicable regulations. The Firm will, always, ensure the highest standards of due diligence to protect its employee and safeguard its brand and reputation.

The Company is committed to the follow:

- Comply with the requirements of the Relevant Laws and appropriate guidelines and licensing terms applicable to the Company being a licensed gaming operator;
- Develop and maintain its AML policies, procedures, systems and controls to prevent opportunities for ML/TF by its customers, vendors and third party intermediaries with whom it conducts any business;
- Allocate responsibility at appropriate levels to ensure compliance with this AML Policy;
- Provide initial and annual training and education programs to ensure all relevant employees and persons acting on behalf of the Company are aware of their personal responsibilities and the procedures to be adhered to;
- Take reasonable measures to verify the identity of any client/vendor/third-party intermediary with whom it conducts/proposed to conduct any business;
- Create a culture of compliance where the standards are set from the top, senior management and lead a culture of compliance and commitment in this regard;
- Resolutely work to reduce the risk of harm from gambling. Invest in and use data, technology and measures to identify harmful play, incorporate protections, intervene early to guard against consumer harm and prevent crime; and
- Innovate to protect and actively identify and manage risk and evidence this at every stage.

- Keep records of relevant documentation and co-operate with any request for information from any Regulatory or Governmental Authority ("**Authority**");
- Report to the relevant Authority where there are reasonable grounds to suspect that a ML/TF offence has been or is suspected to have been committed.

2. REGULATORY FRAMEWORK AND THE BACKGROUND OF AML & CTF REGULATIONS

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. 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.

For guiding principles adopted in this AML Policy, the Company has carefully considered the following Relevant Laws for:

- 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.

Under the Relevant Laws, the term 'Money laundering' is generally defined as engaging in acts designed to conceal or disguise the true origins of proceeds of crime so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets.

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 criminal spending money gained in a bank robbery to gamble in a casino or betting shop.

Money laundering in the eGaming industry, typically, takes place in the following manner:

- Exchanging money that is acquired criminally for money that appears to be 'clean' or 'legitimate' by gambling on low risk outcomes.
- Use of such proceeds of crime to fund gambling as a leisure activity (so called criminal or 'lifestyle' spend)

Where a person intentionally commits, or assists in the commission, of any of the following acts 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 offences.

Criminal property shall mean those derived from the following offences:

- Conversion, transfer or deposit of the proceeds 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 act 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.

If undertaken successfully, ML ultimately provides a legitimate cover for the source of income. Therefore, in layman's terms, ML is considered as conversion of money from "black to white." Money laundering takes place when money obtained illegally (dirty money) is introduced into the financial system, with the objective of making that money look like "clean money" that can be used for legitimate purposes. Criminals attempt to hide or disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction, and the confiscation of criminal funds.

There are three acknowledged phases to money laundering:

- Placement • Layering
- Integration

The broader definition of money laundering offences includes even passive possession of criminal property, irrespective of the amount, as money laundering. 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.

Phase 1 – Placement: The introduction of unlawful cash or other proceeds derived from illegal criminal activity into the financial system through activities such as deposits and wire transfers;

Phase 2 – Layering: The separating of the proceeds of illegal activities from the original source of the funds through the use of layers of financial transactions, such as converting funds to traveller's cheques, money orders, letters of credit, securities or valuable assets such as a home, art, jewellery or precious metals. This stage can also be characterized by a series of complex transactions or movement of funds among accounts and/or financial service providers and the blending of illegal dirty money with legal clean money, which may confuse the audit trail for investigators and provide anonymity (e.g. the sale or switch of holdings in the above unit trust into other forms of investment); and

Phase 3 – Integration: Giving apparent legitimacy to illicit funds by re-integrating them back into the economy through using apparently legitimate transactions such as loans, or merely selling the assets accumulated during the layering stage to allow laundered funds to be disbursed back to the laundering party, appearing to be from a legitimate transaction and usually via a creditable financial organization. (E.g. assembling layered money in an account and using it to set up an investment portfolio).

Terrorist Financing

Terrorist financing involves taking funds that were obtained through legitimate or illegitimate means and utilising the funds to finance terrorism. Terrorist financing is a conversion of money from "white to black." Whilst the funds may not have been illegally gained, the funding, supporting or knowledge of terrorist financing is a criminal offence.

Criminals target entities that do not have the appropriate systems and controls in place to identify and stop money laundering and terrorist financing. Weak controls will allow the criminals to use these entities, albeit unknowingly, to launder dirty money. The aim of this AML Policy is to ensure that the Company has appropriate systems and controls in place to stop the Company from being used to launder money or move and/or launder terrorist funds.

Terrorist financing involves: “the 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 organisations include: -

- Private donations by terrorist supports / sympathisers
- Abuse and misuse of non-profit organisations 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.

Measures to put in place for countering money laundering and combating terrorist financing:

- Streamline player KYC & AML checks at onboarding to drive a competitive experience with automated risk screening and through media searches as well;
- 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; and
- Terrorist financing involves: “the solicitation, collection or provision of funds with the intention that they may be used to support a terrorist act or organization.

Money Laundering Offences

Money laundering is the term used for a number of offences involving the proceeds of crime or terrorism funds. The following acts constitute the act of money laundering:

- Concealing, disguising, converting, transferring criminal property or removing it from the legitimate financial system
- Entering into or becoming concerned in an arrangement which you know, or suspect facilitates the acquisition, retention, use or control of criminal property by or on behalf of another person
- Acquiring, using or possessing criminal property

These are the primary money laundering offences and are thus prohibited acts under the Relevant Laws.

There are several criminal offences which relate to money laundering, principal amongst these being:

- Concealment, disguise, conversion or transfer of “Criminal Property” or removal of it;
- Acquisition, use or possession of criminal property;
- Entering into, or becoming concerned in, arrangements which are known or suspected to facilitate the acquisition, use, retention or control of criminal property by, or on behalf of, another person;
- Tipping off or making a disclosure which is likely to prejudice an investigation; or
- Failure to disclose knowledge or suspicion of money laundering.

Criminal Property is property which constitutes a person's benefit from “Criminal Conduct” or represents such a benefit where the alleged offender knows or suspects that it constitutes or represents such a benefit. “Criminal Conduct” includes, but is not limited to, drug trafficking offences, terrorist activity, burglary and theft, corruption, tax evasion, fraud, forgery, counterfeiting, blackmail, people trafficking, illegal arms dealing, black diamonds and extortion.

Tipping Off is where someone informs a person or people who are, or who are suspected of being involved in money laundering, in such a way as to reduce the likelihood of their being investigated or prejudicing an investigation. A person found guilty of tipping off or prejudicing an investigation offence is liable to imprisonment a fine or both under the Relevant Laws. In addition, a new criminal offence was created whereby, any individual who recklessly makes a statement in the context of money laundering which is false or misleading commits an offence punishable by a fine and or up to two years imprisonment.

Terrorist Financing Offences

Life imprisonment or temporary imprisonment for no less than 10 years may be imposed on whoever:

- Offers, collects, prepares, obtains or facilitates the obtainment of funds for the purpose of using same although aware that they will be used, in part or in whole, in the commission of a terrorist offence.
- Offers funds to a terrorist organization or person or collects, prepares, obtains or facilitates the obtainment of funds for such terrorist organization of person, although aware of the their or purpose.
- Acquires, takes, manages, invests, possess, transmits, transfers, deposits, keeps, uses or disposes of funds or carries out any commercial or financial bank transaction although aware that all or part of such funds are collected as a result of a terrorist offence, owned by a terrorist organization or intended for the financing of a terrorist organization, person or offence.

Sanctions and penalties

The Company will comply with any sanctions, embargos or restrictions in respect of any person or state to which the UN, UK or EU has decided to apply such measures. The below sanction regime will be followed:

<https://www.gov.uk/government/collections/financial-sanctions-regime-specific-consolidated-lists-and-releases>

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>

If the Company breaches any of these sanctions, embargos or restrictions, it will report these to the relevant Authority in accordance with this AML Policy.

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.

3. MLRO – ROLES, RESPONSIBILITIES AND DUTIES

The Relevant Laws require the Company to develop the appropriate compliance management arrangements and designate a MLRO to ensure strict adherence with the AML Policy and the controls put in place by the Company.

The employees shall report to the MLRO on any AML and CTF related discussions, disclosures and matters.

The current MLRO of the Company is: Mr. Rishabh S.

Email id of the MLRO: compliance@gameszapped.com

The MLRO will have direct access to the Senior Management and shall be responsible to ensure this AML Policy, the related procedures and controls and the Relevant Laws and regulations are complied with.

The MLRO's responsibilities shall specifically include:

- 3.1. Ensuring that the Company is in compliance with the Relevant Laws;
- 3.2. Ensuring a speedy and appropriate reaction to any matter in which money laundering or terrorist financing is suspected;
- 3.3. Advising and training Senior Management and staff on developing and implementing internal policies, procedures and controls on AML and CTF;
- 3.4. Promoting compliance with the Company's AML Policy and taking overall charge of all AML/CTF matters within the Company;
- 3.5. Carrying out the day-to-day operations for compliance with the Company's AML and CTF policies, procedures, systems and controls;
- 3.6. Acting as the point of contact to receive information and coordinate requests from employees regarding AML issues;
- 3.7. Submitting suspicious activity report (SAR) to the relevant authority if, following the AML compliance check, the players' funds are known or suspected to have criminal origins;
- 3.8. Establishing SAR procedures and arranging for the maintenance of copies of all underlying documentation;

- 3.9. 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 sanction breaches;
- 3.10. Receiving and acting upon any relevant government, regulatory and international findings, recommendations, guidance, directives, resolutions, sanctions, notices or other conclusions;
- 3.11. Assisting in establishing, developing and coordinating the Company's monitoring procedures for AML purposes;
- 3.12. Taking reasonable steps to establish and maintain an appropriate AML and CTF training program;
- 3.13. Identifying appropriate instances to perform enhanced due diligence on potential clients;
- 3.14. Reviewing and monitoring all transactions and settlements with account holders of a value exceeding GBP 30,000 within a rolling 365-day period and obtaining the relevant enhanced diligence documents for validating source of wealth in such cases, in accordance with the terms of this Policy;
- 3.15. Reviewing the AML Policy on an annual basis to determine its effectiveness and reporting to the Senior Management on the same along with any modifications to the AML Policy and other policies and procedures thereunder;
- 3.16. Coordinating the review and response to AML audit(s).

4. Responsibilities of the Senior Management

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 policy, procedures and controls put in place.
- 4.2. Ensuring 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 Policy, necessary to identify, measure, manage and control the Company's money laundering risks;
- 4.3. Ensure that AML policies, procedures, systems and controls enable the Company to determine whether a customer is a Politically Exposed Person ("**PEP**");
- 4.4. Carry out annual assessments of the adequacy of the Company's AML and CTF systems and controls to ensure that they continue to enable it to identify, assess, monitor and manage money laundering risks adequately;
- 4.5. Ensure that an appropriate employee is designated as a MLRO, at all times to undertake roles and responsibilities set out for MLRO in this AML Policy;

- 4.6. Ensure that employees are adequately trained and comply with the relevant requirements of this AML Policy, and the procedures, systems and controls issued under this.

5. Customer Due Diligence Policy

The Company is required to have and follow reasonable procedures to document and verify the identity of the customers prior to establishing business relationship with them. The CDD procedures set out below address the types of information the Company will collect from the customer and how it will verify the customer's identity. The aim of these procedures and controls is to enable the Company to form a reasonable belief that it knows the true identity of its customers.

5.1. Risk based Customer Due Diligence:

The Company shall use risk-based approaches when undertaking ongoing customer due diligence, in accordance with the RA Matrix. The employees and persons acting on behalf of the Company shall strictly comply with the CDD requirements set out in this AML Policy for opening or operations of any account. No anonymous accounts or accounts in fictitious names shall be permitted, and all individuals opening an account must be over the age of 18.

To ensure checks and verification with the CDD policy, the Company shall use:

- Background screening software which enhances the ability to validate a customer's identity and prevent identity fraud. Additionally, this software risk scores a customer on the basis of their historical play and transactions is used to help identify suspicious activity by customers.
- Acceptable forms of customer identification documents include: any identification carrying the PASS logo (for example passport or citizenship card etc.), a driving licence (including provisional licence) with photocard or a passport.

5.2. Customer Due Diligence Requirements:

The Company shall perform CDD when:

- The Company establishes business relations or conducts any transactions with the customer. In this case the Company shall obtain from the customer information pertaining to their identity as set out in detail below and such information shall be documented for record keeping;
- The Company has doubts about the accuracy and completeness of any information previously obtained.

Documents Verification

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

- ✓ Full name of the customer
- ✓ Unique identification number (Passport, Govt-issued photo ID, etc)
- ✓ Existing mailing and residential address along with the proof thereof

- ✓ Contact numbers
- ✓ Nationality
- ✓ Date of birth

5.3. Document Verification

In case of the documents collected from individual customers as a part of the CDD,

- The passport must:
 - ✓ Be a clean copy detailing the holder's name, date of birth, place of issuance, issuing country, validity, issuance and expiry date, include a clear photograph of the Players, place of birth, have a number, include the holder's signature;
 - ✓ Match details provided by the customer to the Company, including the signature.
- The proof of address must:
 - ✓ Be dated within the last three (3) months, detailing the customer's name and physical residential address;
 - ✓ Match the details provided by the customer to the Company.

In case of the documents collected from corporate customers 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 Company'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 customer's website confirm relevant information given on the application and compares against the documents supplied;

5.4. Ongoing and Enhanced Due Diligence:

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

- In case of bettors with gross settlements of GBP 30,000 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;
- In case the Company has doubts about the accuracy and completeness of any information previously obtained.

The internal monitoring systems and software used by the Company for monitoring transactions by the bettors shall automatically trigger notifications to the MLRO and the senior management in the event the EDD Thresholds set out above are met. 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 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.

The Company should have transactional monitoring programs to support the ongoing/enhanced due diligence in place to identify behavior/ transactions which may be indicative of suspicious behavior. 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.

In such cases, the MLRO shall and the Company shall ensure that the MLRO shall, obtain certified copies of documents pertaining to such account holder's source of funds in the manner set out in this AML Policy.

There are various processes detailed below which when used may increase the confidence that there is no ML or TF concern associated with the customer:

- Third-party verification: use of software or using approved third parties to conduct face-to-face verification of customer documents; for example, in some countries Post Offices provide this service.
- Validation of customer documents: Certified copies of documents to validate name, address, date of birth and source of funds of the customer. For the purposes of validating the source of funds, the Company shall obtain certified copies of the bank statements of the customer or proof of business (business registration/ incorporation certificate).
- Address validation check: Using a secure code delivered to the customer's address to validate that the customer is residing at the address stated.
- Background and lifestyle checks: Using open source research to obtain further information about the customer's source of wealth, occupation, property ownership status and lifestyle.

- Source of funds: Confirm the immediate source from which the funds have derived. For the purposes of confirming the immediate source of funds, certified copies of the bank statements of the customer should be obtained and reviewed.
- Source of wealth: 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.
- Internal corroboration of user identity: This could emanate from a variety of sources from customer monitoring, other databases and face to face verification where possible.

5.5. Politically Exposed Person:

Politically Exposed Persons (PEP) shall mean and include a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business, or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual widely and publicly known (or actually known by the firm) to be a close personal or professional associate of such an individual.

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.

The Company shall use third party service providers and public information, including information available in Internet databases, to determine whether any customer account holder is a PEP. If we discover information indicating that a particular customer may be a PEP, and upon taking additional reasonable steps to confirm this information, the Company determines that the individual is, in fact, a PEP, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer 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 customer 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 Company's policy, it will ensure that it does not enter into relationships with individuals where it is known, or the Company has substantial reasons to believe that funds are derived from corruption or misuse of public assets.

The decision to open an account for a PEP should be taken in discussion with the MLRO and the Senior Management who shall identify the customer and make special arrangement to address the risks associated with such a customer (to ensure that the Company does not unknowingly assist in hiding or moving the proceeds of corruption by senior foreign political figures, their families or associates).

PEP accounts will be subject to more rigorous documentary and other due diligence requirements. Adequate measures will be taken to cater 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);
- Checking source of wealth, type of transactions to be conducted through the account, and jurisdictions involved in such transactions; 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.

6. Risk-based Approach

- 6.1. Background: 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 gambling industry. 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 to ensure effective compliance with the Relevant Laws. The RA Matrix adopts an approach which is proportionate to the risk exposure of the customer. These risks will be evaluated in the context of nature of the Company's business, customers, products, services and any other matters which are relevant in the context of money laundering and terrorist financing.

In order to comply with the Relevant Laws, we are mandated to identify and assess money laundering and terrorist financing risks, and the establish, implement and monitor proportionate policies, procedures and controls to adequately mitigate and manage the risks identified.

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 operator.
- 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 annually monitor and review the RA Matrix adopted by the Company and any changes to the same, shall be adopted in this AML Policy.

- 6.2. Identifying Risks: The Company will undertake a risk-based assessment of every customer, and assign them a risk rating proportional to the money laundering risk posed. High risk accounts should be monitored more frequently and closely. At least once a year, all account risk profiles should be reviewed again. The detailed parameters for categorizing the risk posed by the customers is set out in the RA Matrix.

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

- Identify the customer and any beneficial owner(s);
- 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 customer, its ownership and control structure, and its beneficial ownership (if any), including its possible status as a PEP;
- Take into consideration the customer's country of origin, residence, nationality, and place of incorporation or place of business (if corporate);
- Take into consideration the relevant product, service or transaction with Company.
- The identity of customer, and beneficial owners, as well as persons acting on behalf of customers, shall be verified by using the documents required for completing CDD in the manner set out in this AML Policy.

When relying on other sources 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 customer.

As a part of the Company's policy, no relationship/ account will be commenced unless the customer provides all relevant documents for the risk assessment to the relevant personnel of the Company. Any exception to this rule shall require written approval of the MLRO.

- 6.3. Geography: Establishing the nationality of customers, their bank locations and their employer's location is important to ensure that they are not from a country subject to international sanctions or with ties to higher risk countries. On occasion, establishing the nationality of other individuals or entities closely connected to the individual applicant may be required to assess risk.

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 customers.

Where higher risk countries, which shall be notified by the Company and introduced in the systems control for account opening, 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, employees shall contact the MLRO immediately before proceeding further.

7. Employee Compliance

- 7.1. Employee Obligations and Liabilities: Each employee 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 customers, develop and maintain a clear understanding of their practices, and report activities identified as unusual/suspicious to the MLRO.

- 7.2. Employee Training: One of the most important controls for the prevention and detection of money laundering is to have employees 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 employees 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 (**AML Training**):

- 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 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.
- 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.

The AML Training shall further includes: (1) ways to identify red flags and signs of money laundering that arise during the course of the employee's duties; (2) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis and, where appropriate, the filing of SARs in the manner set out in this Agreement; (3) what employees' roles are in the firm's compliance efforts and how to perform them; (4) the firm's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the Relevant Laws.

Delivery of the AML Training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos etc. The MLRO shall maintain records to show the persons trained, the dates of training and the subject matter of their training etc.

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 part-time or casual employees.

8. Identifying and Reporting Suspicious Transactions

- 8.1. Suspicious Transactions: The Company shall monitor on an ongoing basis, its business relations with every customer, including transactions as well as any other material change in each customer's identification information. The Company shall further, during the course of business relations, observe the conduct of the customer's account and scrutinise transactions undertaken to ensure that the transactions are consistent with the Company's knowledge of the customer, and where appropriate, the source of funds.

The employees 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.

Examples of suspicious activity include the following:

- Transactions which have no apparent purpose and make no obvious economic sense, or which are designed or structured to avoid detection;
- 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 customer, 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 customer refuses to provide information requested without reasonable explanation;
- Where a customer 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 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.

- 8.2. 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 and persons acting on behalf of the Company to the MLRO ("**Internal Report**"). The Internal Report should be documented or electronically recorded. 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. 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.

- 8.3. 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. The Company may also require further information to be obtained from the customer, if necessary. Any approach to the customer should be made sensitively and preferably by someone already known to the customer, to minimise the risk of alerting the customer or an intermediary 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 ("**External Reporting**"). The known or suspected money laundering activity must be reported to the Financial Intelligence Unit of the relevant jurisdiction in which the used in a transaction, which is known or suspected to involve money laundering, is located.
- 8.4. Failing to report: Failing to report suspicious activity under the AML regulatory framework is a criminal offence, which can lead to liabilities to the Company, the MLRO and the employees / persons acting on its behalf. Where employees and/ or the MLRO fail to comply with the obligations to make disclosures as soon as practicable after the information giving rise to the knowledge or suspicion comes to the employee and/ or the Co, they are open to criminal prosecution.
- 8.5. Tipping off, or prejudicing an investigation: Under the Relevant Laws, any employee or persons acting on behalf of the Company shall be deemed to have committed an offence of tipping off, if they:
- Disclose any information regarding the SAR being filed against a person to the MLRO and/ or the relevant regulatory authorities.
 - 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 disposes 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 SAR 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. Reporting & Recording

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

- The results of the review of AML & CTF Measures and AML Training;
- 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;
- 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:

- Assess the report;
- Take action, as required subsequent to the findings of the report, in order to resolve any identified deficiencies; and
- Make a record, in writing, of the assessment and the action taken.

All records shall be kept in line with any regulatory or legal requirements. Destroying or disposing of records without appropriate approval from the MLRO is strictly prohibited. In circumstances where a criminal investigation is being undertaken all records will be kept until the authorities advise otherwise.

The Company shall make and keep certain records and these records shall be kept for a minimum of ten (10) years.