AML/CFT Policy

Effective from: October 2023

Last updated: July 31, 2024

Version: 1.00

1. Policy

Money Laundering and Terrorist Financing are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Individuals involved in Money Laundering and/or Terrorist Financing continually attempting to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such individuals must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

Money Laundering in the online gaming industry manifests itself in two opposing forms:

a) the use of criminal funds to fund gambling activities; and

b) the exchange of criminally acquired funds for legitimate money.

In both cases, authorities fear that those phenomena damage sports, the online gaming industry, and society as a whole. Therefore Money Laundering, when not eliminated, can have far-reaching implications.

Terrorist Financing may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for unlawful purposes. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding e risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures.

The Company takes AML/CFT seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where it operates. The Company’s procedures and internal controls are designed to ensure compliance with all applicable national and international regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

2. Objectives

This Policy outlines the AML/CFT strategy of the Company in order to:

a) ensure that statutory and regulatory obligations to prevent Money Laundering and Terrorist Financing are met, taking positive action to minimize the risk of the Company's products and services being used for the purpose of laundering funds and using proceeds of criminal activity, or Terrorist Financing;

b) ensure that the Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with Money Laundering and/or Terrorist Financing;

c) terminate any relationships where the Account Holder's conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations; and

d) comply with the Company's AML and CFT obligations based on national and international regulations.

3. Scope

This Policy applies to all persons working for the Company or on the Company's behalf in any capacity, including Employees, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external contractors, third-party representatives and business partners, sponsors, or any other person associated with the Company that falls within the scope of the Company's AML Policies.

This Policy defines procedures that will assist all persons working for the Company to comply with its legal obligations. Failure of an Employee to comply with the procedures defined within this Policy may lead to disciplinary action.

4. Regulatory Framework

4.1 National regulations

Pursuant to the the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

a) The National Ordinance on Money Laundering (P.B. 1993, no. 52);

b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together will all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

c) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

d) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);

e) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93); and

f) National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

4.2 International regulations

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing these standards in its national legislation.

On international level, the FATF plays an important role in the combating of Money Laundering and Terrorist Financing and the proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing necessary measures, reviews

Money Laundering and Terrorist Financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating Money Laundering and Terrorist Financing. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present Policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

5. Procedures

In an effort to be compliant with the applicable rules, regulations and international standards, the Company has procedures in place to which it attains itself when providing Services to Account Holders. These procedures cover the following standards:

- Risk management
- Know Your Customer Procedure
- Monitoring of Account Holder activities
- Reporting of unusual transactions
- Recordkeeping

6. Risk Management

6.1 Risk Assessment

The possibility of online gaming being used by criminals to assist in Money Laundering and/or Terrorist Financing poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the Company and/or its Employees. For this purpose, the Company must carefully identify its risks and manage them accordingly.

The Company takes the following steps to manage its risks appropriately:

i. identifying the Money Laundering and Terrorist Financing risks relevant to the Company;
ii. assessing the level of risk;
iii. understanding the impact of the risk;
iv. designing and implementing appropriate policies, procedures and controles to manage and mitigate these risks;
v. monitoring and improving the effective operation of these controls and identifying any weaknesses; and
vi. recording what has been done and why.

In view of the above, the Company must conduct a risk assessment to analyse the risks faced by the Company and ensure that the identified risks are properly mitigated and resources adequately invested.

The risk assessment must identify and analyse the risks related to the following four key risk sources stemming from inherent vulnerabilities in the online gaming sector:

i. Account Holders
ii. Product / service / transactions
iii. Geography

The Company must review its risk management processes on an on-going basis to ensure that it remains abreast of new risks. As a minimum, the risk assessment must be reviewed annually, or more frequently in the case of any important changes to products or technology, payment methods, customer type and other material changes.

The risk assessment will also analyse the policies, procedures and systems of the Company in order to ensure that the identified risks are properly mitigated through the adoption of robust policies and procedures. The results of the risk assessment will serve as the foundation to determine the Company's risk appetite. The following risk areas should be considered by the Company for the purpose of the risk assessment:

Account Holder Risk

The risk of Money Laundering/ Terrorist Financing may vary in accordance with the type of Account Holder. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. An Account Holder having a single source of regular income will pose a lesser risk of Money Laundering/Terrorist Financing than an Account Holder who has multiple sources of income or irregular income streams. PEPs, high spenders and Account Holders with disproportionate spending patterns generally pose a greater risk of Money Laundering/Terrorist Financing.

Product/Service/Transaction

Risk Some products/services/transactions are inherently riskier than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the Account Holder to influence the outcome of a game, be it on his own or in collusion with others. The use of specific funding methods should also be treated as high risk factors. This includes cash and other similar or anonymous payment methods that may not leave or disrupt the audit trail, and allow the Account Holder to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies. The exceptional use by an Account Holder of Player Accounts held or cards issued in the name of third parties is also to be regarded as a high risk factor. Conversely, where an Account Holder

transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of Money Laundering decreases.

Geographical Risk

The geographical risk is the risk posed to the Company by the geographical location, the place of residence and nationality of the Account Holder. The nationality, residence and place of birth of an Account Holder have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organisations operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of Money Laundering/Terrorist Financing. In order to identify and manage potential hazards, the high-risk territories are the next:

i. Prohibited Jurisdictions: these jurisdictions are prohibited under the Curaçao license conditions and/ or pursuant to a resolution of the Company's managing director (Aruba, Belgium, Bonaire, Curacao, France, Netherlands, Saba, Singapore, Statia, St Maarten, USA);
ii. jurisdictions which are identified by the FATF as high-risk jurisdictions subject to a call for action;
iii. jurisdictions under increased monitoring by the FATF;
iv. countries which are identified by the European Union as high-risk countries;
v. countries which are identified by the United States as state sponsors of terrorism.

6.2 Risk Classification

Upon registration, the Company assesses the risk of each Account Holder taking a risk-based approach. The level of due diligence that should be performed on the Account Holder is determined based on the risk classification above.

As PEPs pose a particulary high risk, the Company does not allow PEPs to have a Player Account. Any applicant who is identified as a PEP during the on-boarding stage during, may not open a Player Account. If an Account Holder is determined to be or to have become a PEP at a later stage, his/her Player Account shall be immediately closed.

6.3 Know Your Customer (KYC) Procedure

An individual cannot make use of the Services unless that individual is over eighteen (18) years of age or any legal age at which gambling or gaming activities are permitted under the law or jurisdiction applicable to his person, and has successfully registered for a Player Account. To register for a Player Account, an applicant must register personally and provide the following information:

1. First and last name;
2. Date of birth;
3. Gender;
4. ID card number;
5. Full residential address;
6. Telephone number;
7. Valid email address and
8. Username and a password.

The name on the Player Account must match the true, legal name and identity of the Account Holder. The username, password and other personal information related to the Player Account must be kept secret and confidential and may not be used by any third party. In case of a suspected violation, the Account Holder must request new log-in credentials.

6.4 Due Diligence

Standard due diligence

Standard due diligence is conducted in the following cases:

i. anytime during the Player onboarding;
ii. upon a request for withdrawal; and
iii. anytime at the discretion of the Company.

All applicants are may be required to submit proof of identity, proof of address and payment ID at moment of deposit of funds or where applicable (for further details, see the Terms and Conditions) at any given time requested by the Company. Account holders may be required to submit satisfactory documentation to proof the identity and residential address including but not limited to copies of:

i. valid passport;
ii. identify card;
iii. driving license; and/or
iv. recent utility bill not older than three months.

Depending on the method used for the verification of the authenticity of the documentation, the documents are not required to be certified prior to the provision thereof. Further specifications in relation to the method of verification are to be detailed in separate complementary instruments to this document.

The Company has geo-blocking measures in place that restrict residents of Prohibited Jurisdictions access to the Website. In addition, the Company screens all applicants against international sanctions lists in order to prevent that sanctioned individuals open a Player Account.

The Company will proceed to review the provided information within reasonable time and will contact the applicant and request further information in case the provided documentation is found to be unsatisfactory. A document may be considered unsatisfactory if it is not in English, is suspected to be fraudulent, is suspected to be obtained from a third party to perform illegal operations over the Internet, or for any other reason subject to the discretion of the Company. The applicant may be required to provide further information or information in the internationally accepted format, including but not limited to requesting official translation of legal documents with appropriate seals. If the applicant does not succeed in providing sufficient information, refuses to do so or provides documentation not meeting the criteria (e.g. forged, altered, failing security checks), the Company may immediately proceed to permanently close the Player Account without the refund of the deposited amount.

Enhanced Due Diligence

If at the discretion of the Company, the provided information is considered unsatisfactory or is suspected to be fraudulent or obtained from a third party to perform illegal operations on the site, the Company may engage third party agencies to confirm the provided information on the identity and the payment details.

6.5 The monitoring of Account Holder activities

The Company takes reasonable steps to prevent activities of Money Laundering and Terrorism Financing and constantly monitors all Player activities including financial habits and behavior in order to mitigate industry related risks such as money laundering, terrorism financing and other criminal activities such as fraud.

6.5.1 Unusual activities

The Company has systems in place to monitor the activities on the Player Accounts for the presence of any unusual or suspicious. These activities include but are not limited to:

Duplicate or multiple Player Accounts

Any Player Accounts containing the same personal information, IP address or bank Terrorist Financing is considered to be a duplicate Player Account. It is not permitted for an Account Holder to have duplicate Player Accounts or manage more than one (1) Player Account when using the Services on the Website including but not limited to the web-based version. If the Company becomes aware, suspects or believes that this might be the case it reserves the right to immediately terminate any and all Player Accounts held and the Player Account balances either deemed as forfeited by the Account Holder in which event the deposit will be subject to further investigation by the Company. Any winnings arising from such behavior will be forfeited.

Collusion

Upon the suspicion of the multiple registration by Account Holders acting in collusion or as a syndicate, the set up of fictitious Player Accounts or the use of front men, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close Player Accounts.

Betting strategies

Upon the suspicion of the use of fraudulent betting strategies, such as martingale and arbitrage betting, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close Player Accounts.

Identity fraud

At the detection of any use of falsified documentation (identity fraud), the Company will proceed to close the Player Account(s). Any winnings arising from such activities shall be confiscated and the deposited amount will be subject to further investigation.

6.5.2 Money Laundering Reporting Officer (MLRO)

The Company has designated an MLRO who is in charge of the review of KYC information and the monitoring of Player Account activities and is further assisted by designated personnel. Further, the MLRO is in charge of ensuring that this policy is adhered to, reviewed and maintained regularly.

6.6 Deposits and Withdrawals

All financial transactions must match the name of the credit card or other payment accounts through which the Player Account is funded or money is withdrawn. Any inconsistencies will be considered a breach of the Terms and Conditions. The transaction will be suspended and the Player Account subject to further investigation.

Withdrawal requests can only be addressed to the Account Holder registered on the Player Account and only to the account from which deposits were made. The provided information on the withdrawal form must be identical to the personal data held by the Company. Withdrawal requests made to other parties will not be taken into consideration.

6.7 Transactions using Cryptocurrency

Cryptocurrency transactions are only possible if the initial deposit was made with a crypto currency. Following this transaction all transactions (deposits, wagers and payout) with the Player must be conducted using the same crypto currency as with the first deposit. The Company will at no time sell/buy/exchange crypto currency with and/or to FIAT currency. The Company is bound by the following requirements as set by the *Master License Holder*:

- Collect and verify proof of identity and proof of address as described above in the 'Client Due Diligence' paragraph and to make sure that the Player is over 18 years of age;
- Collection and storage of hardware KYC in all pathways from signup, login, deposits and withdrawals, including but not limited to IP address, mac address and browser information to ensure that all wagering, deposits and withdrawals are to/from the same Player (IP and computer);
- The Company will make available to the Master License Holder on demand and provide proof of balance as acceptable by the Master License Holder, to ensure Player's funds have been deposited; Provide proof of Solvency to the Master License Holder on a periodic basis (weekly, monthly) to ensure that operator has all funds to cover all bets and jackpots and that the crypto currency is kept in a separate account.
- The Company will display the rate of exchange from crypto currencies to FIAT currency on the home page of the Website. In no way shall the Company make exchanges between any crypto currency and any FIAT currency.
- The Company must include in their Terms and Conditions and highlights that crypto currency values can change dramatically depending on the market value.

It is important to note that due to the current anti-money-laundering regulations, the Player may deposit money into the Player Account only in order to play and to use the Services. Likewise, the Player may only withdraw winnings and not the funds deposited into the Player Account. Players who deposit and withdraw without gaming activities will have their funds blocked until further notice. The Company is not a financial institution and does not grant interest on deposits. In any case, the Company reserves the unlimited right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

Notification of new payment methods will be made on the homepage of the Website and sent by e-mail to the Account Holders as they are added. For each new depositing method, this Manual and the Terms and Conditions on the Website will be updated accordingly.

6.8 Ongoing monitoring

The Company reserves the right to conduct a review at any time to validate the identity, age and/or registration data provided by the Account Holder in order to verify the use by the Account Holder of the provided services for any breach of the Terms and Conditions and any applicable laws. At the moment of registration the applicant provides the Company with authorization to make any relevant inquiries pertaining to his person and to use and disclose information to any third party considered necessary in order to conduct its verification checks. Third party agencies may be engaged in an effort to confirm the provided age, identity, address and payment details, the ordering of a credit report and/ or the verification of the provided information by checking it against certain public or private databases. All applicants are made aware that by accepting the Terms and Conditions of the Company, they agree that the provided information may be used, recorded and disclosed and that the data may be recorded by the Company or third party engaged.

The review may be performed from time to time at the discretion of the Company and/or due to regulatory, security or other business reasons. During the review the Account Holder

may be restricted from withdrawing funds from the Player Account and/ or prevented from accessing certain Services offered on the Website.

7. Recognizing and reporting of unusual transactions

Any unusual transactions or circumstances for which the Company has not received sufficient explanation may give rise to its report to the Curaçao FIU. The incidence of one of the following suspicious indicators will be notified by any Employee to the MLRO:

a. the Player does not cooperate in the carrying out of due diligence;
b. the Player attempts to register more than one Player Account with the Company;
c. the Player deposits more than EURO 5,000 /24h by means of multiple prepaid cards;
d. the Player deposits funds well in excess of what is required to sustain usual betting patterns.
e. the Player makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
f. the Player makes frequent deposits and withdrawal requests without any reasonable explanation;
g. noticeable changes in the gaming patterns of a Player, such as when the Player carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out;
h. the Player enquiries about the possibility of moving funds between Player Accounts belonging to the same gaming group;
i. the Player carries out transactions which seem to be disproportionate when seen in the context of what is known about the Player's wealth, income, or financial situation;
j. The Player seeks to transfer funds to the Player Account of another Player or to a bank account held in the name of a third party;
k. The Player displays suspicious behavior in playing games that are considered as high risk.

Upon notification, the MLRO assesses the indicators and decides on whether or not submitting an STR to the FIU. The Company will hold a list of all instances in which it did not consider it necessary to report to the relevant authority. The decision not to report will need to be sufficiently supported. It is prohibited to inform a Player or third parties of the reporting of or the intention to report an activity or transaction to the FIU.

8. Recordkeeping

The Company maintains a record of all relevant documentation on a separate database for at least five years after ending a business relationship. The Company is obliged to retain files in a way that enables investigating authorities to identify a satisfactory audit trail for individual transactions including the amounts, currencies and type of transactions.

In specific circumstances, if ordered by rule of law and permitted by national law and the relevant authorities, the Company may provide copies of the records maintained.

9. Training

In line to ensure the knowledge and awareness of the AML/CFT risks and the efforts conducted by the Company for the prevention thereof, all relevant staff are required to receive training at least once a year. The MLRO is responsible to determine the content of the training events but will ensure the following topics to be discussed:

- Awareness regarding certain topics and aspects concerning the fight, prevention, control and management of risks in relation to money laundering, the financing of terrorism and bribery and corruption amongst others;
- Policies and procedures maintained by the Company regarding the awareness, detection and deterrence of mentioned risks;
- Mechanisms, procedures, controls records and tools maintained by the Company in relation to the subjects discussed.

10. Staff Due Diligence

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates. This information is used to initiate pre-employment checks and screening with the support of third-party screening providers.

11. Periodical review of AML/CFT policies

The AML/CFT policies of the Company are subject to a yearly review, comprising of a fair and unbiased appraisal of each of the required elements of this policy. The review includes testing of internal controls and transactional systems and procedures to identify problems and weaknesses. The review may be conducted by Employee or group of Employees, so long as the reviewer is not the MLRO and does not report directly to the MLRO.