Anti-Money Laundering Policy

CONTENTS

A. Compliance Statement

It is the policy of the Company to comply in all respects with the requirements of the Money Laundering Legislation[1] (including but not limited to the 5th AML Directive[2]) by ensuring that we have policies and procedures to aid compliance.

The main scope of this policy is to establish the essential standards designed to prevent the Company from being used for money laundering and terrorism financing. This Anti-Money Laundering (AML) policy applies to the Company and all of its staff who provide services which might be used to conceal or disguise the true origins of criminally derived proceeds with the intention to make unlawful proceeds appear to have derived from legitimate origins or to constitute legitimate assets.

B. General Obligations

This Policy sets out the procedures which must be followed to enable the Company to comply with its legal obligations. To give effect to this AML policy, the Company is committed to:

(i) Formulate and implement internal rules and develop procedures and systems to detect and monitor suspicious transactions and to report thereon to the relevant authorities;
(ii) Ensure sufficient resources are devoted to the training of staff increase their awareness and ability to deal with suspicious transactions and to keep them informed of new legislative developments and requirements;
(iii) Ensure commercial considerations never override the need to comply with the Regulations;
(iv) Create an environment where staff who report on suspicious transactions can do so confidentially and without fear of reprisal.

C. Definition of Money Laundering and Terrorist Financing

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction and confiscation of the criminal funds. There are three stages in the process:

I. Placement: Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments.
II. Layering: How the link between the funds and the criminal is concealed.
III. Integration: Investing and/or recovering the funds in a way that looks legitimate.

As it is strictly a Company policy not to accept cash as means of payment, the Company's AML Policy is focused to prevent the use of the Company's activities and resources in the 2nd and in the 3rd stage.

D. Money Laundering Reporting Officer (MLRO)

The Company Director, as the nominated Money Laundering Reporting Officer (MLRO), shall receive disclosures about any suspected money laundering or financial terrorism activity and shall be responsible for informing the Company of the AML policies and procedures. The responsibilities of the MLRO is to supervise the actions of the Company and consider the contents of any report made to him/her in relation to relevant information that is available to the Company.

E. Monitoring of Suspicious Activity

[1] For copies of the Act and Regulations, access the Ministry of Justice site at: https://www.gamingcontrolcuracao.org/regulation/aml

The Company will monitor for suspicious activity. If any such suspicious activity is detected, additional due diligence will be performed before proceeding with the transaction. If a reasonable explanation is not determined, the suspicious activity shall be reported to the MLRO. Suspicious Activity includes but is not limited to:

i. The player exhibits unusual concern regarding the terms and conditions of his/her player account, particularly with respect to his/her identity, or furnishes unusual or suspect identification or business documents.
ii. The customer has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
iii. The player displays unusual activity such as large deposits and withdrawals, or deposits and immediate withdrawals;
iv. The player requests winnings to be deposited in another player's account.

The Company will enact a number of policies and procedures which help it to identify such suspicious activity – refer to policies & procedures in sections F to J.

F. <u>Customer due diligence and on-going monitoring</u>

In accordance with Customer Due Diligence measures under the Regeling indicatoren ongebruikelijke transacties – PB 2015, 73, it is the policy of this Company to undertake a risk assessment, and ensure that evidence of customer's identity is obtained and retained as appropriate for all clients.

Due to the nature of the online gaming business, the Company conducts an *enhanced* due diligence process for all of its prospective customers.

- *<u>Notification to customers</u>*

On the Company's website under "terms and conditions" the Company will provide notice to its customers that it may collect certain customer identification information from each customer as well that it is complies to AML regulations. Refer to abstract below;

"The Company complies with the Prevention of Money Laundering Act and Regulations issued thereunder. The Company shall check all transactions to prevent money laundering. The Company shall report any suspicious transaction to the relevant competent authorities. If You become aware of any suspicious activity relating to any of the Games of the Website, You must report this to the Company immediately. The Company may suspend, block or close Your Member Account and withhold funds if requested to do so in accordance with the Prevention of Money Laundering Act."

Before registering an account, the Customer will have to agree to these Terms and Conditions.

- *<u>Required Customer Information</u>*

The Company's KYC procedures will require prospective customers to create a full profile at point of registration.

Mandatory information required at registration stage includes:

(i) true name and surname;
(ii) unique email address;
(iii) phone number;
(iv) date of birth; and
(v) password

This evidence will be obtained before the customer can access the online games. In case that the customer is a Politically Exposed Person (PEP), the customer is considered as high risk and further due diligence procedures is performed at the Company's discretion.

In addition to completing the registration form, the Company may carry out additional verification procedures (such as an ID card or driving licence) for any payout. If necessary, the Company will do a phone verification exercise, which will involve calling the number the user has stated and verify the information provided by the player.

Once all the information requested is obtained, the Company sends a confirmation email to the customer on the email inserted by the customer in the registration form. The player account may be blocked or closed if the requested information or documents, or if such information or documents supplied is/are found false or misleading.

In addition, to the due diligence process performed at initial acceptance stage, the players are monitored on an on-going basis. Internal Controls as per section G provide the framework for on-going monitoring of the players.

G. Internal Controls

Internal control procedures have been designed to comply with the regulations. Internal controls take the form of manual controls implemented on a daily basis by Company's Operations Team (and/or Payments Team) and computer/automated controls inherent within the gaming system software.

The gaming system has inbuilt internal control tools which based on the information inputted by the prospective customers can trigger red flags about suspicious activity to the Operations Team. Refer to some examples below:

i. ***Prevention of multiple accounts held by same user:*** Inbuilt system checks confirm whether the email provided by the prospective customer is unique in the customer database preventing the possibility of a player having multiple accounts. If a player tries to open more than one account, for whatever reason, the Company reserves the right to block or close any or all of the player's accounts at its discretion;
ii. ***Detection of any underage registrations:*** Under age registrations are automatically not allowed by the system;
iii. ***No cash and no credit policy:*** Credit card deposits are accepted by the system only if the customer enters a valid credit card number with sufficient funds. A player can participate in any game only if the player has sufficient funds on his/her Member Account for such participation. It is the Company's policy not to accept cash and not to give any credit whatsoever for participation in any game;
iv. ***Withdrawal is only allowed if the name of person requesting the withdrawal is the same name of person holding the bank account:*** The Company's policy is that it shall only affect payout to an account, card, wallet or similar instrument in the name of the player receiving payout. Under no circumstances shall the Company affect a payout to a player in a name other than in the name of the player.

Internal controls are not entirely computer dependent. The Operations Team also has an important part in detecting and preventing money laundering. The below are a number of controls operated by the Operations Team:

i. On-going monitoring and assessment of player's risk indicators and changes in players patterns;
ii. On a daily basis a deposits report is reviewed by the payment and risk department and follow ups made on suspicious transactions and manually entered deposits;
iii. Monitoring of large deposits and withdrawals and/or deposits and immediate withdrawals;
iv. All withdrawals are approved by a member of the Payment Department;

v. The Operations Team confirm that the name of person requesting the withdrawal is the same name of person holding the bank account. Suspicious credit card deposits, transactions and accounts are followed up by a verification process;
vi. Customer log activity is regularly analysed for indications of suspicious activity;
vii. Operations team also prepares weekly and monthly high level reports for review by top management.

Additional verification on suspicious deposits, transactions or accounts will include but not limited to:

a. Call Player to verify Telephone Number, take note of player response/phone manner in call. This call is made by Support Staff in the same language of the player account.
b. Check if player exists on local country phone book, tax records, electoral register, additional public databases, with the same information.
c. Request ID, Proof of Address, copies and statements of credit cards.

H. Reporting (Internal & External)

The Company's policy is that any knowledge or suspicion of money laundering activities must be immediately reported to the MLRO. Refer to specimen of Internal Reporting Form in Appendix 1.

On receipt of the report, the MLRO reviews the contents of internal reports, requests further information when required and then decides on the appropriate action to be taken. It also Company's policy that each decision, in respect of each and every report received, needs to be recorded (Refer to specimen in Appendix 2).

MLRO files a Suspicious Transaction Report (STR) if he suspects or has reasonable grounds to suspect that;

(i) a transaction may be related to Money Laundering (ML) or Funding Terrorism (FT), or
(ii) a person may have been, is, or ,may be connected with ML/FT;
(iii) or ML/FT has been, is being, or may be committed or attempted.

The STR is drawn up by the MLRO as soon as reasonably practicable, but not later than 5 working days from when the suspicion first arose.

The Company strictly prohibits any *tipping off* by its personnel to players. Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. Under no circumstances shall any officer, employee or appointed agent disclose or discuss any AML concern, investigation, notice or filing of the suspicious activity report with the person or persons subject of such, or any other person, including members of the officer's, employee's or appointed agent's family.

I. Record Keeping

It is Company policy to maintain the following records;

- a copy of, or the references to, the evidence of the client's identity obtained; and
- the supporting evidence and records in respect of the business relationships and occasional transactions which are the subject of customer due diligence;
- internal reports of MLRO and external reports made to the FIU;
- records of AML training provided to employees.

Records are maintained for a period of 5 years, beginning on the date on which the business relationship ends.

J. Communication and Training

The Company commits itself to ensure that all personnel are provided with training on detection and treatment of transactions that may relate to money laundering. The level of training provided to an employee is appropriate according to the employee's role and responsibilities within the Company.

Training of AML is directed to ensure that the Company's employees are;

i. Able to identify a suspicious transaction;
ii. Know the procedure to follow if such circumstances are encountered;
iii. Know the provision of the relevant law and regulations with respect to ML/FT;
iv. Be able to identify PEPs and perform proper KYC.

This AML manual is also available to all personnel of the Company.

K. Risk assessment and Compliance management

It is the policy of the Company to undertake a risk assessment for all clients and retain such assessment for a period of 5 years after we cease to act for the client.

The Company shall review this policy on an annual basis or earlier if so required by amendments made to the respective laws or if requested by the FIU and/or other relevant authorities.

COMPANY NAME

Signature: _____

Name: _____

Title: _____

Date: _____

Appendix 1: Internal Suspicious Money Laundering Transaction Report Specific to Employees to be submitted to the Money Laundering Reporting Officer

Instructions for completion of the form

It is your legal duty and a requirement of your employment with this practice that you report any knowledge or suspicion concerning money laundering to the firm's MLRO.

In accordance with our internal procedures, you need to complete the report form as quickly as is practical. Should any delay be likely you need to contact the MLRO immediately.

The form should be completed and sent to the e-mail address – Compliance@xcm.cw. Please do not take any copies.

Tipping off is a criminal offence. You should therefore avoid discussing your suspicions or concerns with anyone other than the MLRO in all but the most unusual circumstances.

Failure to comply with these requirements may result in action being taken against you in line with the Company's usual disciplinary procedures.

To: **The Money Laundering Reporting Officer**
Date of the report: [Insert date]
Prepared by: [Insert name and position]
Name & Player ID of individual(s) suspected: [Insert name of all individuals suspected]
Name & Player ID of client (if different): [Insert client name or confirm that no difference from the list above]
Reason for suspicion: [Give a detailed description of the reasons for your knowledge or suspicions. Please include supporting documentation if applicable]
Date suspicion first aroused: [insert date]
Names of all other colleagues who have been involved with this client's affairs: [Insert name of all individuals informed – each of whom should sign the declaration below]

Declaration

I am aware of the risks and penalties regarding "tipping off", or investigation of the above or related matters by the authorities.

Name:	Signed:	Dated:

Appendix 2: Form to be completed by the Money Laundering Reporting Officer upon receiving the above report from an Employee

Date received _____

Consideration of Disclosure:

Action Plan:

Outcome of Consideration of Disclosure:

Are there reasonable Grounds for suspicion?

Is consent required from the Financial Intelligence Unit (FIU) to any ongoing or imminent transactions which would otherwise be prohibited acts? ☐ YES ☐ NO

If YES, please record authorisation and "way forward" details received from the Financial Intelligence Analysis Unit

If there is reasonable grounds to suspect Money Laundering, but you do not intend to report the matter to the FIU, please set out below your reasons for non-disclosure

Signed _____ Dated _____

THIS REPORT SHALL BE RETAINED FOR A MINIMUM OF FIVE (5) YEARS