Anti-Money Laundering and Counter-Terrorism Financing Compliance Policy

Nuxgen B.V.

1. Introduction

1.1. Nuxgen B.V. ('**Nuxgen**' or the '**Company**'), a legal entity, duly incorporated under the laws of Curacao, that operates under the License No. 1668/JAZ issued by Curaçao eGaming, Authorized and Regulated by the Government of Curacao, is committed to carry out its business activity in an honest and ethical manner. This commitment includes complying with all applicable laws and regulations aimed at combating money laundering ('**ML**') and terrorist financing ('**TF**'). This Anti-Money Laundering ('**AML**') Compliance Policy ('**Policy**') has been developed by the Company to reduce the risk of ML / TF or any other criminal activity associated with its business in gambling industry and distribution of its products/provision of services.

1.2. This Policy provides for information and guidance on how to recognize and deal with ML / TF issues.

1.3. ML is the process by which criminally obtained money or other assets (criminal property) are exchanged for 'clean' money or other assets with no obvious link to their criminal origins. Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. It also covers money, however come by, which is used to fund terrorism.

1.4. This Policy has been adopted having regarded to the fact that Company is engaged into B2B activities only and does not provide services/distribute products to individuals.

2. Objectives of the Policy

2.1. The Company will endeavor to keep itself updated with developments both at national and international level on any initiatives to prevent ML / TF.

2.2. The Company will conduct business exclusively with clients who are involved in legitimate business activity and whose funds are derived from legitimate sources and make every effort to prevent using of Company's activities by the clients for ML/TF purposes.

2.3. This Policy has been adopted in order to make the Company constantly vigilant to prevent ML / TF and, consequently, minimize and manage reputational, legal, financial, cyber and transparency risks.

2.4. This Policy is intended to assist its employees, contractors, and other third parties acting on the Company's behalf in understanding of FATF Recommendations together with other applicable anti-money laundering and counterterrorist financing laws ('**AML Laws and Guidance**') and to support them in making the right decisions that will be in line with the Company`s corporate position described in this Policy.

3. Nuxgen`s obligations

3.1. In order to meet the AML Laws requirements, the Company has a responsibility to:

a) appoint a person employed or engaged by a services agreement as the designated Money Laundering Reporting Officer ('**MLRO**') whose responsibilities will be in line with those required by the AML Laws and Guidance;

b) implement and maintain a procedure on the reporting of suspicious activity and transactions;

c) take reasonable actions to establish the identity of any legal entity with whom the Company contemplates entering into business relations using risk-based approach to 'Know Your Client' ('**KYC**') procedure and client due diligence ('**CDD**') programme;

d) provide the Company`s employees / engaged persons with regular training in the identification and reporting of client`s activity that gives grounds for suspecting ML / TF;

e) maintain identification and transactional documentation as set forth in AML Laws and Guidance;

f) cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity;

g) not to enter into business relations with clients potentially engaged in any activity that might lead to a breach of this Policy.

3.2. The prevention, detection and reporting of ML / TF constitutes the responsibility of all workers employed at the Company together with all persons working for the Company or under its control ('**Workers**'). All these persons are required to avoid any activity that might lead to or suggest a breach of this Policy.

4. Internal procedures

Know Your Client ('KYC') programme

4.1. For the purposes of mitigating potential ML / TF risks presented by its clients, the Company carries out identification and verification procedures using risk-based KYC approach composed of three main components: (1) Client Identification Programme ('**CIP**'), (2) Client Due Diligence ('**CDD**') procedure; (3) Enhanced Due Diligence ('**EDD**') Programme.

4.2. These procedures should be performed for the purposes of (1) identifying and verifying the client's identity; (2) obtaining details of the purpose and intended nature of business relations; (3) conducting ongoing monitoring of business relations; and must be carried out in the following cases:

a) at the time when the Company establishes business relations with the client for the first time;

b) where there is reason to believe that previous actions carried out on an existing client are inadequate;

c) where the client`s identifying details have been changed;

d) where there are reasonable grounds to presume that the third person is purporting to act on behalf of the client;

e) where there are reasonable grounds to presume that the client is engaged in ML / TF.

4.3. In the course of KYC programme, CIP and CDD are considered as mandatory review stages for general procedure conducted in respect of each Company`s client. Data received during CIP and CDD should, among other, be used to

identify the level of client`s risk and the necessity to request additional information within EDD procedure.

4.4. **CIP (identification)**

4.3.1. CIP is aimed to identify and verify the identity of the Company`s prospective clients, which may be potentially involved in ML / TF activities and transactions. This programme should apply with respect to each prospective client before entering into business relations.

4.3.2. Identification process implies collection of the following client`s information:

a) full legal name, legal form, identification number and relevant document confirming client`s registration;

b) documents regulating client`s activity (e.g. statute and formation documents – memorandum / articles of association) together with relevant list of directors and their place of residence;

c) government-issued gambling license;

d) registered office or at another location notified to the company registry;

e) e-mail address and telephone number;

f) client`s bank details.

4.4. **CIP (verification)**

4.4.1. In accordance with this Policy, the Company should at the time of entering into business relations with the client verify its identity, including but not limited to its name, identification number, address by means of referring to publicly-available resources (e.g. government websites, third-party databases etc.).

4.4.2. The Company is under obligation to keep in electronic form all records and originals made / provided in the course of identification and verification of the client identity for at least five years from the date of the client`s most recent transaction / transaction attempt.

4.5. **CDD procedure**

4.5.1. In addition to basic client`s information collected within CIP identification and verification processes, the Company should clarify with the client the following:

a) source of funds;

b) expected product usage;

c) corporate ownership structure, including identification of the client`s beneficial owner (e.g. its name, date of birth, identification number, address, mobile phone, place of residence, valid passport) and information on ultimate parent.

4.6. The questionnaire for CIP and CDD procedures is provided in "Due Diligence Form" separately drawn up by the Company.

4.7. The completed questionnaire as well as all other documents and information received in the proves of CIP identification & verification + CDD procedure should be provided to MRLO for assessment.

4.8. **EDD procedure**

4.8.1. Based on the results of verification and identification procedures conducted in the context of CIP and CDD programmes, MRLO evaluates and assigns to the client the level of ML / TF risk it potentially possesses (Low, Medium, High). This risk rating of the client will determine whether and to what extent implement EDD and additional controls. Please note, that high-risk clients must be subject to an EDD process as required by local regulations.

4.8.2. The potential indicators of the medium and high-risk clients may, among other, include the following:

a) residents of countries included in the EU List of non-cooperative jurisdictions;

b) unlicensed gambling legal entities;

c) clients organized, domiciled, or doing business in "high-risk jurisdictions" according to FATF list;

d) clients whose beneficial owners could not be identified and reasonably confirmed or politically exposed persons ('**PEP**');

e) legal entities whose funds appears to have its source from corruption or activities that are illegal in Curacao or in the country of origin;

f) legal entities whose identities are not known or cannot be identified in the course of due diligence procedures;

g) legal entities whose source of funds cannot be explained;

h) legal entities, their representatives and / or beneficial owners are on embargo or included in terrorist list issued by EU, OFAC or local authorities;

i) legal entities together with beneficial owner or anyone associated with them have handled the proceeds from crime;

j) clients subject to significant negative news, as identified through screening and due diligence activities;

k) a client's business formation documents are from a tax haven, or a country that poses a high risk for ML / TF, or a country that is not logical for the client;

l) suspiciously close ties to government officials and PEPs, previous allegations of corruption or unethical behavior;

4.8.3. The specific list of additional information within EDD varies in each particular case and depends on the level of client`s risk and peculiarities of its business activity (e.g. financial statements; information regarding purpose and intended nature of the business relationship etc.).

4.8.4. The results of EDD procedure should be submitted to MLRO, which draws up the client`s risk profile, decides on the necessity to request additional information from client and whether to pursue business relationship inter se.

Perspective clients who MLRO deems to pose unacceptable ML / TF risks may be rejected.

4.9. **Monitoring of the Client`s Suspicious Activity**

4.9.1. The Company exercises monitoring of client's activity related to Company's products/services purchased by such clients in order to detect activity which is unusual or suspicious compared to the client`s risk profile (and that may potentially lead to ML / TF activity).

4.9.2. Typical signs of ML / TF activity include, *inter alia*, the following:

a) the client orders services/products from the Company, which are (1) complex or unordinary large; (2) without any apparent logical, legal and economic purpose (e.g. loss-making transaction where the loss is avoidable); (3) out of the ordinary range of services normally requested; or (4) is outside the experience of the Company in relation to this particular client;

b) client`s refuse to proceed with the transaction when asked for identification without any reasonable explanation;

c) methods or volumes of payment that are not consistent with the payment policy or that are not customarily used in the course of business, e.g., payments with money orders, traveler's checks, and / or multiple instruments, and payments from unrelated third parties without any reasonable grounds;

d) there are no sound economic or lawful grounds for the clients requesting Company`s products / services;

e) large amount of cash being used;

f) payment to or from countries considered high risk for ML / TF;

4.9.3. All Workers of the Company should be aware of the above ML / TF indicators, which may raise suspicions in potential ML / TF activities. Please, note, that the above list is not exhaustive given new techniques constantly developed by criminals. Thus, the Workers need to remain vigilant and use their experience and judgment in determining activities

which may serve as a sign of ML / TF, paying due consideration to the factors reflecting deviation from the client`s and acceptable business practice.

4.9.4. In case of any suspicion, the Company`s Workers have to report it to MLRO. MLRO is also under obligation to report on such suspicious transaction to the competent authority of Curacao. If the MLRO gives the consent to proceed with a provision of services / supply of products, it applies exclusively to that specific transaction. If the client requests further activities or transactions, further consent is required from the MLRO even if, to the Worker`s mind, there are no grounds for suspicion.

5. Training

5.1. In order to assure the effectiveness of instructions, procedures and processes as well as Worker`s general understanding of AML due diligence procedures, the Company develops AML compliance training programmes (e.g. on-class trainings, webinars) obligatory to all Workers. The content of such training programmes has to be elaborated according to trainees` roles and responsibilities on at least annual basis.

5.2. The Company also requires all new employees to become familiar with relevant AML compliance requirements pertaining to their specific job functions and to receive the most updated information.

6. Non-Compliance

6.1. All Workers are responsible for understanding this Policy and undertaking any specified responsibility assigned to them.

6.2. Workers, failing to comply with this Policy, should be subject to disciplinary actions, which may result in dismissal.

6.3. Those Workers who fail to comply with the AML Laws and Regulations may also be subject to civil and / or criminal penalties and imprisonment according to the applicable legislative requirements.

6.4. Non-compliance with this Policy and AML Laws and Guideline could also cause significant damage to the reputation of the Company and its staff. Failure by a Worker may also expose the Company to penalties, censure and enforcement actions by the respective authorities.

7. Other provisions

7.1. This Policy should be reviewed on at least annual basis as part of the Company`s overall risk management process. The Company will also review this Policy when:

a) there are any major changes in the law or practice concerning AML / CTF actions;

b) the Company has identified the weakness in this Policy;

c) there are changes in the nature of the Company`s business, its clients or other changes which impact on this Policy.

7.2. MLRO is available for consultations on the interpretation and administration of this Policy.