**Anti-money laundering**

**1-Anti-money laundering Manual Overview**

1.1-Objectives and Scope

As part of its continuous improvement implementations, Rex Star Corp N.V. is dedicated to putting in place the necessary steps needed to ensure that all employees, full-time or contractual, participate actively in preventing any of the Company's services and/or outlets for the sole or partial purpose of money laundering and/or the financing of terrorist undertakings.

Money Laundering (ML) and the use of legal or illegal monies for the purpose of terrorist financing have become ever growing threats – Rex Star Corp N.V. (referred to herein as the "Company") is fully committed to playing its role in assisting the international fight against such organized crime and terrorism.

The Company has therefore incorporated the following Anti-Money Laundering and Terrorist Financing Policy ("Policy") as part of its internal process. The Company has applied this Policy to all its employees and adheres to the highest of the industry's best practices in its mission to prevent any possible criminal activity through money laundering.

The Company's AML program is designed to be compliant with applicable legislation, regulations and directives which include but not limited to, among others, and with the following:

- Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering.
- EU Regulation 2015/847 on information accompanying transfer of funds.
- Various EU Regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods.
- European Business Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash.
- FATF Recommendations for International Standards on combating Money Laundering and the financing of terrorism and proliferation (AML/CFT)

1.2-Money Laundering Defined

Money Laundering is the terminology used for a number of illegal offences encompassing

money obtained from certain crimes, (such as extortion, insider trading and drug trafficking, tax avoidance and false accounting) as "dirty" and needs to be "cleaned" to appear to have been derived from legal activities, so that banks and other financial institutions will deal with it without suspicion. The International Monetary Fund (IMF) had defined the offence in its official website as a process by which the illicit source of assets obtained or generated by criminal activity is concealed to obscure the link between the funds and the original criminal activity

Money can be laundered by many methods that vary in complexity and sophistication.

Whether it be through conversion, transfer of property, concealment, disguise, acquisition or possession of funds derived from criminal activity or the participation/assistance of the movement of funds derived from criminal activity in order to appear legitimate – are all forms of money laundering.

### 1.3-Distribution of the AML Policy

This AML Policy has been reviewed and approved by the Executive Management Team. The Policy will be provided to all staff (frontline, leads, managers and owners) and will be redistributed if updated.

The Compliance Officer is responsible for providing a report to the Executive Management team for review not less frequently than once every twelve (12) months asto the effectiveness of the Policy and related operational procedures, and shall provide recommendations to management as to proposed operational or policy enhancements.

The Executive Management team shall review the content of this Policy for necessary updates not less frequently than once every twelve (12) months. Recommendations and feedback will be given to the Compliance Officer. With the exception of directives from relevant authorities, any proposed amendments to the Policy require the review and approval of the Compliance Officer, the Executive Management team and legal counsel.

## 2-COMPLIANCE OFFICER – MONEY LAUNDERING REPORTING OFFICER (MLRO)

### 2.1-Appointment of the Compliance Officer/MLRO

A qualified senior employee shall be appointed at all times as Compliance Officer. The Compliance Officer has been identified and the Compliance Officer’s contact details made available to all staff and applicable staff of service providers.

## 2.2-Reporting Structure and Independence

The Compliance Officer holds no other position within the organization or any affiliated company or supplier and operates independently from all other functions within the organization in order to ensure that actual or perceived conflicts of interest do not occur.

Subject to oversight by the UBO, the Compliance officer has the authority to act independently from other functions within the organization in order to fulfill his/her below noted roles and responsibilities. The Compliance Officer has the full and public support of the executive management team in executing his duties. All staff are required to assist the Compliance Officer (and the nominated officer, as appropriate) in fulfilling their duties.

## 2.3-Duties and Responsibilities of the Compliance Officer/MLRO

AML Compliance Officer is in charge of financial regulations and personal data compliance requirements, making sure the company's AML policy corresponds to the international system. Further the MLRO is responsible for oversight and management of all compliance related functions within the Company and within its affected suppliers, including the protocols described in this Policy. Compliance Officer/MLRO duties include (but not limited to) the following:

- Ensure that procedures are in place to ensure compliance with all applicable legislation, regulations and all associated guidelines, codes of practice and Company policies and procedures;
- Report to the CEO and inform senior management the result(s) of any remedial action taken;
- Attend regular Compliance Meetings with selected senior management, prepare an agenda therefor, and to take, circulate and maintain the minutes thereof;
- Update and maintain any compliance-related policies, including this Policy;
- Plan and co-ordinate training activity for all departments to include key regulatory areas including the significance of regulatory compliance as a whole, ID and age verification, fraud, anti-money laundering, and problem gambling;
- Be the point of contact with the involved Regulator(s);
- Investigate and report any breaches of the applicable laws, regulations, guidelines,

codes of practice and company policies and procedures to senior management and, as appropriate, to the Regulator;

- Plan and co-ordinate training activity for all departments to include key regulatory areas including the significance of regulatory compliance as a whole, ID and age verification, fraud, anti-money laundering, and problem gambling;
- Consult with staff representatives and attend staff meetings on compliance topics;
- Manage regular reviews of Company's internal control system to ensure that it

  accurately reflects the then current operation of the business – and report any discrepancies/oddities to relevant senior management.
- Looking after records of high-risk clients and report suspicious activities, if any.
- Assisting the implementation of an Anti-Money Laundering program of an organization.
- Arranging inspections from third-party organizations and eliminating mistakes in the program, if any.

**3–FIRM POLICY AND COMMITMENT**

The Company will ensure it has appropriate policies and procedures in place to complement this AML policy, in compliance with applicable regulations and recommendations from international and European approved organizations and bodies and monitoring of adherence to those policies will also take place.

Staff members are trained in AML processes, awareness and procedures in accordance with the latest regulatory evolutions and will actively participate in preventing the services of the Company from being exploited by criminals for money laundering or terrorist financing purposes.

The objectives of this and related policies are:

- Ensuring the Company is compliant with all applicable laws, statutory instruments of regulation;
- Protecting the Company and its staff as individuals from the risks associated with breaches of the law, sanctions, regulations and supervisory requirements;

- Preserving and protecting the Company's reputation against the risk of reputational damage presented by implication in money laundering and terrorist financing activities;

- Making a positive contribution to the fight against crime and terrorism.

**4–SCREENING AND MONITORING**

AML screening is performed to fulfil three main objectives.

- Make risk assessment

- Avoid violating sanctions

- Protection from regulatory fines

4.1-Account Screening

AML Account - Name Screening is one of the methods used for risk assessment of existing or potential customers of organizations under the AML obligation.

Upon a customer's account opening process, a preliminary screening both automated and manual will be conducted to identify potentially linked or other suspect account activities compared to the customer profile. The main purpose of the company is to control their existing and potential customers in sanctions, PEP, banned lists, wanted lists, and adverse media data in order to obstruct false positives and false negatives by classifying their customers according to their risk levels and also for the company to be protected from regulatory penalties as well as to avoid violating various sanctions.

As risk levels of customers change over time the company would regularly check the risk level of their existing customers with screening. The company will be maintaining an updated record of customers by performing online verification on them. All AML procedures, policies and controls are regularly reviewed and updated to ensure that they take into consideration new risks that may arise.

Such screening searches for potentially suspect elements, including:

- Accounts that may depict similar information;

- Two or more accounts utilizing the same email address upon creation;

- Customer has more than one account;

- Any other suspicious information / activity identified or suspected by the Fraud or Financial Services teams.

In the event that any of the foregoing screening identifies potential issues, the Financial Services team is notified automatically and will investigate and will enforce applicable business and regulatory rules accordingly. Such business rules may result in a variety of potential risk mitigation steps, including closure of account, escalation to the Fraud team for enhanced diligence, limitation of deposit or withdrawal methods, imposition of deposit limits, etc.

4.2-Enhanced Due Diligence (EDD)

In certain cases, there is the possibility certain customer relationships and large transactions demonstrate higher AML or fraud risks to the Company. In such instances and in addition to its regular customer due diligence protocols, the Company shall carry out Enhanced Due Diligence ("EDD") for further risk investigation. Risky customers and transactions pose a greater risk to the financial sector and cannot be detected by Customer Due Diligence ("CDD") procedures. In this case, EDD procedures will be applied in order to create a higher identity assurance by taking the customer identity and addressing and evaluating the customer's risk category.

During the enhanced due diligence process, the Company will take additional required steps in order to aid the identification of a potential customer, including (but not limited to) personal and financial background. This may involve obtaining additional evidence in verifying the individual in question.

This may include obtaining evidence to verify particular aspects of the customer's identity and verified confirmation in order to establish the source of funds of the customer. The Company's Fraud Detection agents have access to a variety of tools through its suppliers and databases which are used to verify submitted documentation (e.g. Drivers Licenses, and Passports).

The circumstances that may trigger additional concern and may require Enhanced Due Diligence (EDD) are noted below:

- The customer or potential customer is situated in a country of territory that does not apply to the Company's geographical market.
- The customer or potential customer is situated in a country blacklisted to fund or

support terrorist activities.

- The customer or potential customer is or appears to be a Politically Exposed Person or close spouse or family member (see below).

- Any other circumstances as Company reasonably perceives to be a high risk of money laundering or terrorist financing.

The company associates solely with trusted and approved Payment Service Providers whom all have effective AML policies in place as to prevent the large majority of suspicious deposits from taking place without proper execution of KYC procedures onto the potential customer.

4.3–Politically Exposed Person “PEP”

A PEP (Politically Exposed Person), is an individual who currently or previously held a prominent public function in any country. A wide range of persons may be considered as PEPs, including heads of state, senior members of the judiciary, senior military officers and immediate family members of such persons.

Although there is no global definition of a politically exposed person, the Financial Action Task Force (FATF) defined a PEP as “an individual who is or has been entrusted with a prominent public function.” Although the term varies by jurisdiction, along with screening requirements imposed by local financial authorities, most financial authorities separate PEPs into three categories:

- Foreign: Individuals who are elected to political positions or who are appointed to prominent public roles or functions in a foreign country should be classified as foreign PEPs for AML/CFT purposes. Foreign PEPs may be heads of state, cabinet members, government officials, military officers or members of the judiciary. They may also be senior executives of state-owned corporations or important members of political parties.

- Domestic: Individuals who are elected to political positions or appointed to prominent public roles within their country of residence are classified as domestic PEPs. Like foreign PEPs, the domestic category includes heads of state and other foreign government officials, members of political parties, members of the military, members of the judiciary and senior executives.

- International: Senior management employees (or individuals of an equivalent level) who are entrusted with prominent functions by international organizations may be classified as international PEPs.

A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

If an account is identified as a potential match to a PEP list, the account shall be immediately frozen pending escalation and review. The Compliance Officer is immediately notified and a further assessment is made. Enhanced due diligence measures will be applied which involve not only available customer-submitted information but checks of existing PEP lists and a range of news sources, including online and traditional media outlets. The Compliance Officer will reach out to the appropriate department and offer his/her recommendations regarding the account.

4.4-Reporting

If for any reason the Company reasonably suspects that a client and/or an account might be involved in any form of activity that amounts or is connected with money laundering, the Company will immediately inform the required and appropriate external authorities.

If the Company believes that there is some degree of suspiciousness after a transaction has taken place and after an internal investigation confirms as such - the Company will freeze the account and will inform the relevant authorities immediately and disclose all the necessary information at the company's possession required by law to do so. The Compliance officer or an authorized staff will report the activity through the appropriate AML reporting form and submit it to the Regulator or any other competent officer.

Additional reporting procedures are put in place in order to mitigate the Company's exposure to various forms of money laundering and sanctions. These consist of in-house and third-party reporting/monitoring tools that run daily and weekly. Furthermore, AML reporting procedures such as Suspicious Activity Reporting (SARs) and Significant Transaction Reports (STRs) will be conducted and submitted when necessary to the Regulators and also to the appropriate law enforcements should this is required.

4.5-Ongoing and Continuous Monitoring

The Company implements and monitors all activities of clients and/or staff, to ensure that all activities – whether it be transactional or instructional, be consistent and given the required attention for the detection of possible money laundering or terrorist financing.

The Compliance Officer/MLRO will supply the appropriate AML training (which may consist of in-class, video conference, literature and seminars) in order to provide the involved staff, guidelines and direction on:

- The process in reporting suspicious activity;
- Risk Management practices;
- Identification and Verification Procedures;
- Suspicious transaction identification and reporting;
- Record Keeping;
- The type of activity that should be considered significant and critical in detecting possible money laundering – these may be given in class or reading materials;
- Distinguishing specific incidences that may require cause for re-assessment of a risk-based approached;
- The Company consistently implements monitoring processes with the addition of potentially new and future products and/or services it provides to its clients;

Implementations and assessments are put in place (and adjusted if required) in order to mitigate any possible risk of money laundering or terrorist financing where the use of new products and/or services may be vulnerable to. These include but not limited to the following,

  - Overview analysis of transactions over specific periods;
  - Overview analysis of new services/products used by the client;
  - Applying limits to activities on new products/services used by the client for a given time;
  - Requests for justification of noticeable irregular activity from the client.

**5–ACCOUNT - IDENTITY VERIFICATION**

5.1-Account - Identity Verification Requirement

As an identity verification measure, the company must identify and verify its customers to flag potentially risky users and monitor for suspicious activity. Verification processes are designed to help reduce the risks of illicit activity by identifying customers and verifying that this identity is correct. In doing this, suspicious characters and potentially high-risk users can be flagged and monitored, or banned.

Identity theft is a big problem in online gambling. Users can fraudulently obtain credit card details and use these payment methods to enter games using someone else's funds. Equally, users can submit fraudulent documents, playing under other people's identity to avoid the repercussions from terrible losses.

Perhaps one of the most damaging forms of fraud for online casinos is multiple account fraud, where users create fake accounts to throw games.

This procedure forms an integral mechanism for protecting the company from malicious actors and financial crime as well as ensuring that the company is complying with AML regulations.

In order to effectively meet the above mentioned required elements the company implemented an ID and Account Verification process for all of the users and customers in order to ensure and confirm that the details of the users and customers registered are correct and correspond to the particular individual and also to confirm that the payment details and methods used are not stolen or used by someone else, which is to create the general framework for the fight against money laundering and financing terrorism.

5.2–Verification Process

Upon the creation of a new account every customer be allocated a player ID number and will need to enter his/her basic details such as name, address, age, payment method, accept the Terms and Conditions and confirm that he/she is 18 or over and have read and understood the Terms and Conditions of the site(s).

When the account is created, full Identity verification has to be performed and the following have to be provided:

1. Full Name – scan of passport (photo and cover page), driver's license, or national ID card.

2. Nationality – passport or national ID card
3. Gender
4. Date of Birth
5. Full Address - recent utility bill, phone bill, bank statement or council tax bill
6. Payment Method – scan of the front and back of the card used to fund your account, or your bank statement

Full ID verification/re-verification will also be required in the following situations:

- When you deposit or request to withdraw above a nominated threshold – $2000 (Two Thousand Dollars) and more. This can be in one withdrawal, or cumulatively from the time of your first withdrawal. Until the verification is complete the withdrawal or deposit request will be on hold.
- If the address of your first deposit method does not match the address you used to register your account.
- If there is a change in the pattern of your deposits or withdrawals.
- When a name matches, or is similar to that of someone with a history of criminal activity.

Further, when you deposit or request to withdraw $5000 (five thousand Dollar) or more the user will be requested to declare and submit evidence of his source of wealth (SOW). Until the verification is complete the withdrawal or deposit request will be on hold.

Examples of SOW include the following:

1. Ownership of business
2. Employment
3. Inheritance
4. Investment
5. Family

It is critical that the origin and legitimacy of that wealth is clearly understood. If this is not possible an employee may ask for an additional evidence and / or information.

The account will be frozen if the same user deposits either this amount at once or by multiple transactions. An automatic email will be sent to the particular customer or user guiding him through the particular procedure.

In order to fast track the process, the user can upload or email the required documents to the payment team in advance of any request. Account verification will vary according to every individual circumstance. It can take as long as a few days or as little as a few minutes.

## 6-RISK MANAGEMENT

In order to deal with the different risks and different states of wealth in different regions on the earth the company will categorize every nation in three different regions of risk.

### 6.1- Region one: Low Risk

For every nation from region one the Account - ID verification process will be affected as described in section 5.2 above.

### 6.2-Region two: Medium Risk

For every nation from region two the ID- Account verification will be applicable at a lower deposit and/or withdrawal limits. Specifically, ID-Account verification process will be triggered after depositing or withdrawing requests of $1000 (One Thousand Dollars).

For any deposit and/or withdrawal requests exceeding $2500 (Two Thousand Five Hundred Dollars), the user will be requested to declare and submit evidence of his source of wealth (SOW).

Users from a low risk region that change crypto currency in any other currency will be treated like user/customers from a medium risk region and the above ID-Account verifications will be applicable.

### 6.3-Region three: High Risk

Regions of high risks will be banned. High risk regions will be regularly updated to keep up with the changing environment of a fast-changing world.

### 6.4-Enterprise-wide risk assessment

As part of its risk-based approach, the company has conducted an AML “Enterprise-wide risk assessment” (EWRA) to identify and understand related risks specific to the company. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the websites offer. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank’s operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on the company’s understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The EWRA is yearly reassessed.

6.5-Money Laundering Risk Assessment

The crucial purpose of Money Laundering Risk Assessment is to identify the general and specific money laundering risks that the company is facing, determining how these risks are mitigated by the company’s AML program controls and establishing the residual risk.

As a result, the Company is aiming to:

- Identify gaps or opportunities for improvement in its AML policies, procedures and processes;
- AML compliance programme aligns with its risk profile;
- Develop risk mitigation strategies including applicable internal controls and therefore lower its business line residual risk exposure;
- Awareness of the key risks, control gaps and remediation efforts;
- Assist senior management with strategic decisions in relation to commercial exits and disposals;
- Assist management in ensuring that resources and priorities are aligned with its risks;

**7-KNOW YOUR CLIENT (KYC)**

Formal Identification of users and customers on registration and entry into commercial

relations is a mandatory requirement for increasing security and protection against fraud.

The Company requires this procedure as it forms part and parcel of gambling responsibly along with fraud and financial crime prevention – and required by the legislation.

Upon the registration of a new account, the Company will check that you are over 18 years of age and they will verify that you are who you say you are, (a process called Know Your Customer 'KYC').

7.1-Identification Procedure

A copy of your passport, ID card or driving license, each shown alongside a handwritten note mentioning six random generated numbers. Also, a second picture with the face of the user/customer is required. The user/customer may blur out every information, besides date of birth, nationality, gender, first name, second name and the picture in order to secure their privacy.

**NOTE:** All four corners of the ID and/or passport have to be visible in the same image and all details has to be clearly readable, besides the named above. We might ask for all details if necessary.

An employee may do additional checks if necessary, based on the situation.

7.2-Proof of Address

Proof of address will be done via electronic checks, which use two different databases. If an electronic test fails, the user/customer has the option to make a manually proof of address.

A recent utility bill, phone bill, bank statement or council tax bill sent to your registered address, issued within the last 3 months or an official document made by the government that proofs your full address of residence.

To make the approval process as speedy as possible, please make sure the document is sent with a clear resolution where all four corners of the document is visible, and all text is readable.

For example: An electricity bill, water bill, bank statement or any governmental post addressed to you.

An employee may do additional checks if necessary, based on the situation.

## 8-MANAGEMENT OF COMPLIANCE AND AML POLICIES

It is the Company's policy to monitor its compliance program with legal and regulatory AML/CFT requirements. The Policy will be reviewed annually and amendments added accordingly, when new products and/or implementations are applied.

The effectiveness of the Company's AML/CFT program is regularly evaluated to ensure it remains current and is aligned with business activities, regulatory developments, industry standards and best practices. By doing so, the Company adheres to all applicable laws and regulatory requirements in the jurisdictions in which it operates.

## 9-CONTACT DETAILS

For any general inquiries regarding our policies, please contact us via the following email: support@playtron.bet

For complaints the verification process relating to your Account and your Person please contact us via the following email: support@playtron.bet