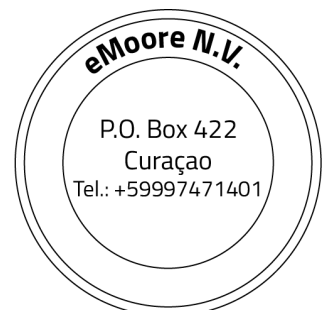


# Casiworx N.V.

## AML MANUAL

Signature: *C. Drommond*  
Name: C. Drommond, Proxyholder of eMoore N.V.



V. 1.0 - MAY 2025

# Table of Contents

|                                                           |           |
|-----------------------------------------------------------|-----------|
| REVISION HISTORY .....                                    | 3         |
| DEFINITIONS AND ABBREVIATIONS .....                       | 3         |
| <b>1. AML/CFT POLICY .....</b>                            | <b>8</b>  |
| 1.1 POLICY.....                                           | 8         |
| 1.2 OBJECTIVES .....                                      | 9         |
| 1.3 SCOPE .....                                           | 9         |
| <b>2. REGULATORY FRAMEWORK .....</b>                      | <b>9</b>  |
| 2.1 NATIONAL REGULATIONS.....                             | 9         |
| 2.2 INTERNATIONAL REGULATIONS .....                       | 10        |
| <b>3. PROCEDURES .....</b>                                | <b>11</b> |
| 3.1 RISK MANAGEMENT .....                                 | 11        |
| 3.1.1 Risk assessment .....                               | 12        |
| 3.1.2 Customer Risk Assessment.....                       | 14        |
| 3.2 KNOW YOUR CUSTOMER PROCEDURE.....                     | 15        |
| 3.2.1 Due Diligence.....                                  | 16        |
| 3.2.2 Client Risk Classification .....                    | 18        |
| 3.3 THE MONITORING OF ACCOUNT HOLDER ACTIVITIES .....     | 19        |
| 3.3.1 Unusual activities.....                             | 19        |
| 3.3.2 Deposits and Withdrawals.....                       | 20        |
| 3.3.3 Transactions using Cryptocurrency.....              | 21        |
| 3.3.4 Ongoing monitoring .....                            | 22        |
| 3.4 REPORTING OF UNUSUAL TRANSACTIONS .....               | 22        |
| 3.5 RECORDKEEPING .....                                   | 23        |
| <b>4. MONEY LAUNDERING REPORTING OFFICER (MLRO) .....</b> | <b>23</b> |
| <b>5. TRAINING .....</b>                                  | <b>23</b> |
| <b>6. STAFF DUE DILIGENCE .....</b>                       | <b>24</b> |
| <b>7. PERIODICAL REVIEW OF AML/CFT POLICIES .....</b>     | <b>24</b> |
| <b>CONTACT INFORMATION.....</b>                           | <b>24</b> |

## REVISION HISTORY

| Version # | Effective Date | Approving Official | Responsible Office  | Next Review Date | Comments |
|-----------|----------------|--------------------|---------------------|------------------|----------|
| 1.0       | May 28, 2025   | eMoore N.V.        | Compliance function | May 28, 2026     | -        |

## Definitions and Abbreviations

|                |                                                        |
|----------------|--------------------------------------------------------|
| Account Holder | An individual who has a Player Account on the Website. |
|----------------|--------------------------------------------------------|

|                                                                      |                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Anti Money Laundering<br>("AML")                                     | All efforts focused on the prevention of money laundering, the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.                          |
| Caribbean Financial Action Task Force ("CFATF")                      | An organization of states and territories of the Caribbean territory that have agreed to implement common countermeasures against money laundering and terrorism financing. ( <a href="http://www.cfatf-gafic.org">www.cfatf-gafic.org</a> ) |
| Combatting terrorist financing<br>("CFT")                            | All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.                                                                                                          |
| Combatting proliferation of weapons of mass destruction<br>("CPWMD") | Efforts aimed at combatting the financing or provision of funds for the sale, transfer, or export of nuclear, chemical or biological weapons, their delivery systems and related materials.                                                  |
| Cryptocurrency                                                       | Distributed, open-source, mathematically based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include Bitcoin, Ethereum, Litecoin and Dogecoin.              |
| Cryptocurrency transaction                                           | The deposit and withdraw of cryptocurrencies into and out of a Player Account held by a Player.                                                                                                                                              |
| the Company                                                          | Casiworx N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 163922.                                                                             |
| Employee                                                             | Any person working for the Company.                                                                                                                                                                                                          |

|                                                |                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Financial Action Task Force<br>("FATF")        | An intergovernmental organization dedicated to developing standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. ( <a href="http://www.fatf-gafi.org">www.fatf-gafi.org</a> ) |
| Financial Intelligence Unit<br>("FIU")         | Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of suspicious transaction reports (STR) and other information regarding potential money laundering or terrorist financing.              |
| Know Your Client<br>("KYC")                    | Know Your Client, the mandatory process of identifying and verifying the client's identity when opening a Player Account and periodically over time.                                                                                                                                                                                                        |
| Money Laundering<br>("ML")                     | A process through which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise, or attempt to disguise, such proceeds to make them appear to be legitimate.                                                                                                                                          |
| Money Laundering Reporting Officer<br>("MLRO") | Designated individual in charge of the review of KYC information and the monitoring of Player Account activities. The MLRO might further be assisted by designated personnel.                                                                                                                                                                               |
| Player                                         | Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened providing him/her with a unique code.                                                                                                                                                    |
| Player Account                                 | An account granted to an individual after registration on the Website. The Player Account is created and issued by the Company and is required for wagering with real money. Only one Player Account is permitted per person, per IP address, per family and per Shared Environment.                                                                        |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Politically Exposed Person<br>("PEP") | A person entrusted with a prominent public function, such as a senior political figure. Individuals closely related to this person, for instance immediate family                                                                                                                                                                                                                                                                                                                             |
|                                       | members and close associates, are also considered PEPs. PEPs are classified as a Money Laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.                                                                                                                                                                                                                                                                     |
| Prohibited Jurisdictions              | Jurisdictions prohibited under the Curaçao license conditions by the Curaçao Gaming Authority at a certain moment, jurisdictions restricted by decision of the Company's managing director at a certain moment when and where still applicable, as well as countries mentioned on the FATF blacklist or on which any financial sanctions has been imposed by the EU/ U.N. and/or the OFAC.                                                                                                    |
| Proliferation Financing<br>("PF")     | The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. |
| the Regulator                         | The Curaçao Gaming Authority (CGA). The regulator for the entire gaming industry operating in and from Curaçao.                                                                                                                                                                                                                                                                                                                                                                               |
| Shared Environment                    | An environment that has a common internet connection which includes but is not limited to airplanes, households, universities, libraries, cyber cafes, coffee shops and offices. Only one Player Account is permitted per Shared Environment.                                                                                                                                                                                                                                                 |

|                            |                                                                                                                                                                            |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service                    | the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.                                         |
| Terms and Conditions       | The terms and conditions for the use of the Services, as published on the Website.                                                                                         |
| Terrorism Financing (“TF”) | The process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities. |
| Website                    | the online gaming platform offering online gaming services operated by the Company.                                                                                        |

# 1. AML/CFT Policy

## 1.1 Policy

Money Laundering, Terrorism Financing and proliferation of weapons of mass destruction 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 ML and/or TF continually attempt 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.

ML 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 ML, when not eliminated, can have far-reaching implications.

TF 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 TF 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. PFWMD may involve the sale, transfer, export, of weapons of Mass destruction, like nuclear weapons and atomic weapons. Such proliferation must be countered as well due to it posing a signification threat to international peace and security, as identity by relevant United Nations Security Council Resolutions (UNSCRs). Therefore, the CP measures involve identifying and assessing the risks of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. 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.

## **1.2 Objectives**

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

- a) ensure that statutory and regulatory obligations to prevent ML and FT are met, taking positive action to minimize 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 ML and/or TF;
- 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, CFT and CPF obligations based on national and international regulations.

## **1.3 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.

# **2. Regulatory Framework**

## **2.1 National regulations**

Pursuant to 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 the following:

- 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.2024, no.41(N.G.2017, no.92)(NORUT) together with 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. 2024 no.41 (N.G. 2017, no. 99) ) (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.
- g) National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- h) Kingdom Sanction Act (N.G. 2016, no. 54);

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.

## **2.2 International regulations**

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

On an international level, the FATF plays an important role in the combating of ML, TF and PF. The FATF monitors the progress of its members in implementing necessary measures, reviews ML and TF techniques and countermeasures, 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 the financing of terrorism. 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.

### **3. 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

#### **3.1 Risk Management**

The possibility of online gaming being used by criminals to assist ML and/or TF 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 ML and TF 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 controls 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.

### 3.1.1 Risk assessment

The possibility of online gaming being used by criminals to assist ML and/or TF 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 conducted a comprehensive risk assessment consisting of a Business risk assessment and a Customer risk assessment to identify its risks and manage them accordingly. In line herewith, further specific procedures are drawn up to further describe the processes that need to be in place.

#### 3.1.1.1 Business risk assessment

The following table outlines the identified risks, the corresponding risk category as well as their likelihood and potential impact during the course of business and the risk score.

| Risk ID | Risk                                                  | Risk Category      | Likelihood | Impact | Risk score (LxI) |
|---------|-------------------------------------------------------|--------------------|------------|--------|------------------|
| R001    | Breach of licensing terms in any jurisdiction         | Regulatory & legal | 4          | 5      | 20               |
| R002    | Failure to comply with AML/CTF regulations            | Regulatory & legal | 5          | 5      | 25               |
| R003    | Non-compliance with responsible gambling regulations  | Regulatory & legal | 4          | 4      | 16               |
| R004    | Advertising violations                                | Regulatory & legal | 3          | 4      | 12               |
| R005    | High player payout rates reducing profit margins      | Financial          | 3          | 4      | 12               |
| R006    | Cash flow liquidity issues                            | Financial          | 4          | 5      | 20               |
| R007    | Fraudulent chargebacks                                | Financial          | 4          | 3      | 12               |
| R008    | DDoS attack disrupting platform access                | Cybersecurity      | 3          | 5      | 15               |
| R009    | Data breach or data loss                              | Cybersecurity      | 4          | 5      | 20               |
| R010    | Unauthorized access to customer data                  | Cybersecurity      | 3          | 5      | 15               |
| R011    | System outages or downtime during peak events         | Operational        | 3          | 5      | 15               |
| R012    | Dependence on third-party software or platforms       | Operational        | 4          | 3      | 12               |
| R013    | Poor internal controls over betting limits or bonuses | Operational        | 2          | 4      | 8                |
| R014    | Entry of a dominant competitor in key market          | Market             | 4          | 4      | 16               |

|      |                                              |                      |   |   |    |
|------|----------------------------------------------|----------------------|---|---|----|
| R015 | Decline in consumer trust in online gambling | Market               | 3 | 5 | 15 |
| R016 | Reduced customer retention                   | Market               | 3 | 4 | 12 |
| R017 | Negative media coverage or scandals          | Reputation           | 4 | 5 | 20 |
| R018 | Social responsibility criticisms             | Reputation           | 3 | 4 | 12 |
| R019 | Players developing gambling addiction        | Responsible Gambling | 3 | 5 | 15 |
| R020 | Failure to intervene with at-risk players    | Responsible Gambling | 2 | 4 | 8  |
| R021 | Poor performance of software vendors         | Vendor               | 3 | 4 | 12 |
| R022 | Payment processor instability or failure     | Vendor               | 4 | 4 | 16 |

### Mitigation strategy and residual risk

The following tables show the mitigation strategy to be implemented and the effectivity rate, followed with the activities to reduce residual risk, the residual risk score and the residual risk level.

| Risk ID | Mitigation Strategy                                    | Mitigation control effectiveness |
|---------|--------------------------------------------------------|----------------------------------|
| R001    | Regular audits, engage local counsel                   | 12                               |
| R002    | Automated monitoring tools, staff training             | 15                               |
| R003    | Self-exclusion tools, RG team                          | 10                               |
| R004    | Ad approval workflow, legal review                     | 7                                |
| R005    | Game RTP analysis, betting limits                      | 7                                |
| R006    | Liquidity reserves, cash forecasting                   | 12                               |
| R007    | Payment verification systems, fraud detection software | 7                                |
| R008    | Cloudflare, WAF, redundancy                            | 9                                |
| R009    | Encryption, multi-layer security                       | 12                               |
| R010    | Role-based access control, 2FA                         | 9                                |
| R011    | Load testing, cloud infrastructure                     | 9                                |
| R012    | SLA enforcement, redundancy plans                      | 7                                |
| R013    | Control dashboards, alerts                             | 5                                |
| R014    | Brand differentiation, loyalty programs                | 10                               |
| R015    | Transparency campaigns, PR management                  | 9                                |
| R016    | Personalized offers, CRM automation                    | 7                                |
| R017    | Crisis communication plan                              | 12                               |
| R018    | Fund RG programs, public reports                       | 7                                |
| R019    | Monitoring, self-exclusion tools                       | 9                                |
| R020    | Behavior tracking algorithms                           | 5                                |
| R021    | Performance KPIs, backup vendors                       | 7                                |
| R022    | Multiple PSPs, weekly performance review               | 10                               |

| Risk ID | Activities to reduce Residual risk | Risk score (LxI) | Residual risk score | Residual risk level |
|---------|------------------------------------|------------------|---------------------|---------------------|
|---------|------------------------------------|------------------|---------------------|---------------------|

|      |                                                                            |    |    |        |
|------|----------------------------------------------------------------------------|----|----|--------|
| R001 | Continuous license compliance training, implement internal reviews         | 20 | 8  | Medium |
| R002 | Enhance KYC processes, deploy AI for transaction monitoring                | 25 | 10 | Medium |
| R003 | Audit RG tools quarterly, include customer feedback                        | 16 | 6  | Medium |
| R004 | Implement retention journeys, feedback loops with frequent users           | 12 | 5  | Low    |
| R005 | Build trust with player protection features, transparency dashboards       | 12 | 5  | Low    |
| R006 | Introduce real-time liquidity dashboards, diversify revenue streams        | 20 | 8  | Medium |
| R007 | Analyze competitor promotions, improve personalization engine              | 12 | 5  | Low    |
| R008 | Set up DDoS scrubbing service, automate scaling responses                  | 15 | 6  | Medium |
| R009 | Conduct periodic penetration testing, enforce data classification policies | 20 | 8  | Medium |
| R010 | Apply anomaly detection for access patterns, monitor admin activities      | 15 | 6  | Medium |
| R011 | Use high-availability architecture, incident response planning             | 15 | 6  | Medium |
| R012 | Use player interaction scoring, initiate guided interventions              | 12 | 5  | Low    |
| R013 | Implement regular vendor reviews, renegotiate SLAs                         | 8  | 3  | Low    |
| R014 | Perform market SWOT analysis, adjust promotional strategies                | 16 | 6  | Medium |
| R015 | Assess vendor dependency, contractual penalties for downtime               | 15 | 6  | Medium |
| R016 | Develop reputation resilience strategy, engage media consultants           | 12 | 5  | Low    |
| R017 | Media monitoring, train spokespersons, prepare PR statements               | 20 | 8  | Medium |
| R018 | Fund responsible gambling campaigns, issue public responsibility reports   | 12 | 5  | Low    |
| R019 | Install automated alert systems, limit manual overrides                    | 15 | 6  | Medium |
| R020 | Perform regular PSP reliability audits, diversify payment options          | 8  | 3  | Low    |
| R021 | Automate detection of addictive behaviors, player nudges                   | 12 | 5  | Low    |
| R022 | Onboard backup payment partners, conduct stress tests                      | 16 | 6  | Medium |

### 3.1.2 Customer Risk Assessment

The Customer Risk Assessment assesses the risk the Company faces when offering its services to a player. As follows an overview of the identified risks.

| Risk ID | Risk                                             | Likelihood | Impact | Risk score (LxI) |
|---------|--------------------------------------------------|------------|--------|------------------|
| CR001   | Onboarding of Politically Exposed Persons (PEPs) | 3          | 5      | 15               |
| CR002   | High spenders without clear source of income     | 3          | 4      | 12               |
| CR003   | Anonymous or incomplete customer KYC             | 4          | 4      | 16               |
| CR004   | Use of cryptocurrency for deposits               | 3          | 5      | 15               |
| CR005   | Structuring or unusual transaction behavior      | 4          | 5      | 20               |
| CR006   | Use of prepaid/gift cards                        | 3          | 4      | 12               |
| CR007   | Multiple linked accounts circumventing controls  | 3          | 4      | 12               |
| CR008   | Customers from high-risk jurisdictions           | 3          | 5      | 15               |
| CR009   | Self-excluded individuals trying to re-register  | 2          | 3      | 6                |
| CR010   | Use of proxy or VPN to mask location             | 4          | 4      | 16               |
| CR011   | Frequent chargebacks or disputed transactions    | 3          | 4      | 12               |

|       |                                                        |   |   |    |
|-------|--------------------------------------------------------|---|---|----|
| CR012 | Inconsistent user behavior suggesting account takeover | 3 | 5 | 15 |
|-------|--------------------------------------------------------|---|---|----|

### Mitigation strategy and residual risk towards AML risk

The following tables show the mitigation strategy to be implemented and the effectivity rate.

| Risk ID | Mitigation Strategy                                                | Mitigation control effectiveness |
|---------|--------------------------------------------------------------------|----------------------------------|
| CR001   | EDD, SOF/SOW checks, PEP list screening                            | 9                                |
| CR002   | Income verification, affordability checks                          | 7                                |
| CR003   | Tiered onboarding, ID verification, biometric authentication       | 10                               |
| CR004   | Crypto wallet KYC, blockchain analysis, transaction limits         | 8                                |
| CR005   | Real-time transaction monitoring, behavior-based alerts            | 12                               |
| CR006   | Restrict use of prepaid methods, EDD thresholds                    | 7                                |
| CR007   | Device fingerprinting, anti-multi-account systems                  | 8                                |
| CR008   | Geo-blocking, EDD for high-risk countries, risk profiling          | 9                                |
| CR009   | Shared exclusion lists, ID verification, behavioral monitoring     | 3                                |
| CR010   | Block known proxy IPs, detect VPNs, additional KYC                 | 10                               |
| CR011   | Limit refund frequency, monitor payment patterns                   | 7                                |
| CR012   | Behavioral analytics, device change alerts, step-up authentication | 9                                |

The following table displays the activities to be conducted to reduce residual risk. The residual risk score is provided as well as the residual risk level

| Risk ID | Activities to reduce Residual risk                                          | Risk score (LxI) | Residual risk score | Residual risk level |
|---------|-----------------------------------------------------------------------------|------------------|---------------------|---------------------|
| CR001   | Automated PEP screening, periodic KYC updates                               | 15               | 6                   | Medium              |
| CR002   | Integrate Open Banking APIs, flag risky customer profiles                   | 12               | 5                   | Medium              |
| CR003   | Enforce expiry-based deactivation, frequent reminder workflows              | 16               | 6                   | Medium              |
| CR004   | Integrate blockchain tracing tools, limit use by high-risk customers        | 15               | 7                   | High                |
| CR005   | Machine learning models for velocity detection and layered transactions     | 20               | 8                   | Medium              |
| CR006   | Cap prepaid card deposits, collaborate with issuers for suspicious patterns | 12               | 5                   | Medium              |
| CR007   | ML-based clustering, manual review of overlapping profiles                  | 12               | 4                   | Medium              |
| CR008   | Review and update high-risk country lists, real-time geolocation alerts     | 15               | 6                   | Medium              |
| CR009   | Centralized exclusion database, tighter re-onboarding criteria              | 6                | 3                   | Low                 |
| CR010   | Deploy VPN/proxy detection tools, require manual verification               | 16               | 6                   | Medium              |
| CR011   | Monitor for fraud patterns, blacklist frequent abusers                      | 12               | 5                   | Medium              |
| CR012   | Trigger step-up verification on anomalies, lock compromised accounts        | 15               | 6                   | Medium              |

## 3.2 Know Your Customer 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:

- a. First and last name;
- b. Date of birth;
- c. Gender;
- d. ID card number``;
- e. Full residential address;
- f. Telephone number;
- g. Valid email address and
- h. Username and a password.

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

### **3.2.1 Due Diligence**

#### **3.2.1.1 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.
- iv. When a transaction or incidental transaction of XCG 4000 or more takes place.

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

- a. valid passport;
- b. identify card;
- c. driving license; and/or
- d. 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. In case the Company discovers that a

transaction in the course of the business relationship of an amount of XCG 4.000 or more takes place, then the Company must perform verification of the Account holder's identity prior to accepting more transactions of the Account holder taking place.

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 sanctioned individuals from opening a Player Account.

The Company will proceed to review the information provided within a reasonable time and will contact the applicant and request further information in case the documentation provided 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.

#### **3.2.1.2 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 will engage third party agencies to confirm the provided information on the identity and the payment details. This process entails but is not limited to the following actions:

- i. verifying the disclosed details against certain (public or private) databases (e.g. sanction lists)
- ii. ordering a credit report
- iii. bank statement showing the initial deposit.

The Company reserves the right to restrict the Account Holder from withdrawing funds from the account and/or prevent access to all or certain parts of the services.

Failure to pass the checks may result in permanent closure of the Player Account and suspension of any of the outstanding balance

### 3.2.1.3 Politically Exposed Persons

Situations involving PEP require the application of EDD measures, independently of the outcome of the risk assessment. This entails having to determine whether a client is a PEP or otherwise and, should this be the case, apply of the following pre-established EDD measures:

- i. Obtain senior management approval to service the PEP;
- ii. Establish what is their source of wealth and, where applicable, their source of funds; and
- iii. Conduct enhanced on-going monitoring of the Account Holder's activity.

Screening for PEP status has to be carried out regularly but it is important that this is done within thirty days of the XCG 4.000 threshold being met. Should an Account Holder who had not been identified as a PEP at on-boarding stage result to have become one, the Employee is required to carry out or implement the measures described in paragraph (i) to (iii) above within the thirty (30) day window, failing which it would have to terminate the business relationship with the said Account Holder.

Information required to determine whether a Account Holder (or its beneficial owner) is a PEP can be obtained either from the Account Holder himself (e.g. by completing a standardized self-declaration as to his status and, to the extent which may be applicable, that of his beneficial owner) or by using reliable electronic databases to screen their Account Holder database. However, where the Employee relies on the Account Holder to disclose and declare whether he is a PEP or otherwise, he is required to (a) provide the Account Holder with guidance as to what is meant by a PEP, including by providing him with a definition of the said term; and (b) confirm on a risk sensitive basis the information so obtained.

### 3.2.2 Client Risk Classification

Upon registration, the Company makes a risk classification for each Account Holder.

The Company maintains the following risk classification:

- Low risk
- Medium risk
- High risk

The level of due diligence that should be performed on the Account Holder is determined based on the risk classification above.

| Type of Account Holder | Monitoring frequency |
|------------------------|----------------------|
|------------------------|----------------------|

|                                                                                                                                                                |                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Account Holders who are under active investigation or suspected in ML/TF or other fraudulent activity and their accounts are not limited for deposit or logins | Daily                                        |
| PEPs, which are deemed to present a high risk                                                                                                                  | Daily                                        |
| High-Risk Account Holders, High-Rollers, PEPs with lower relative risk and active Account Holders from high-risk jurisdictions                                 | Weekly (or upon a material change)           |
| Medium Risk Account Holders                                                                                                                                    | Every six months (or upon a material change) |
| Low Risk Account Holders                                                                                                                                       | Annually (or upon a material change)         |

### 3.3 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.

#### 3.3.1 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 account is considered to be a duplicate 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 setup 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.

#### *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 amount deposited will be subject to further investigation.

### **3.3.2 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.

#### Deposits

An Account Holder is only permitted to use its personal information and personal bank account. The information provided on the deposit form must be identical to the pertaining data held by the Company.

An Account Holder may deposit money in his Player Account only in order to play on the Website and use the Services and is not allowed to withdraw without prior wagering activity.

Furthermore, the Company will not grant interest on deposits. The Company reserves the right to apply certain restrictions to the payment methods in selected countries and/or for certain Players.

#### Withdrawals

An Account Holder can only make a withdrawal request once the initial deposit amount is fully used, and specific bonus terms of a bonus must be satisfied before requesting its withdrawal. No withdrawal will be processed, and funds cannot be withdrawn from the Player's Player Account until: (i) the required verification checks have been satisfactorily completed; (ii) payments have been confirmed; and (iii) the Player has complied with any other withdrawal conditions, specific rules and promotional terms relating to the Player's use of the Website and/or affecting his/her Player Account (for example, any applicable bonus terms), and (iv)

wagering activity has been conducted by the Player in a minimum amount to be further determined by the Compliance function.

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 information provided 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.

### **3.3.3 Transactions using Cryptocurrency**

In those cases where Player requests payment in Crypto, the following will be applicable.

Crypto 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 will further conduct the following procedure:

- 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 maintain and provide proof of balance (as may be acceptable by the Regulator) to ensure Player's funds have been deposited. The Company will make this available to the Regulator on demand;
- Provide proof of Solvency as per the requirements of the Regulator on a periodic basis (weekly, monthly or as deem fit by the Regulator), 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 highlight 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 might need to be updated accordingly.

### **3.3.4 Ongoing monitoring**

The Company reserves the right to carry out a review of the Player Account at any time to confirm the identity, age and/or registration details provided by the Account Holder, in order to ensure that the Customer's use of the services complies with the Terms and Conditions and all 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 information provided may be used, recorded and disclosed and that the data may be recorded by the Company or engaged third party.

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.

## **3.4 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 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.

### **3.5 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.

## **4. 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.

The MLRO is in charge of the following:

- i. ensure a proper review of the Player Accounts by the personnel in relation to identification and verification of an Account Holder,
- ii. keep a list of registered Account Holders;
- iii. monitor the reviews and investigations conducted by the designated personnel performed on the Player Account activities;
- iv. provide initial and ongoing training to all relevant staff ensuring awareness of their personal responsibilities and the procedures in respect of identifying Players, monitoring Player activity, record-keeping and reporting any unusual/suspicious transactions;
- v. cooperate with all relevant administrative, enforcement and judicial authorities in their endeavor to prevent and detect criminal activity; and
- vi. ensure that this policy is adhered to, reviewed and maintained regularly.

## **5. Training**

In order to ensure the knowledge and awareness of the AML/CTF 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.

## **6. 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.

## **7. 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 an Employee or group of Employees, so long as the reviewer is not the MLRO and does not report directly to the MLRO.

## **Contact Information**

For any questions regarding this policy, please contact:

eMoore N.V. Legalcompliance  
Department  
Groot Kwartierweg 10, Livestrong Building  
Willemstad, Curaçao  
Telephone: +599 9 7471401  
Email: [legalcompliance@the-emgroup.com](mailto:legalcompliance@the-emgroup.com)