



ANTI-MONEY LAUNDERING, ANTI-TERRORISM FINANCING AND DUE DILIGENCE POLICY

Key Information

Approving Official(s): Head of Legal

Responsible Office: Head of Legal

Effective Date: 1 January 2025

Next Review Date: 2 January 2026

1. Policy Statement

iMoon B.V. (hereinafter "Company", "iMoon" or "Website") is registered under the Commercial Register of Curaçao under registration number 158383, with an office address at Dr. H. Fergusonweg 1, Willemstad, Curaçao, duly licensed through a sublicense granted by Antillephone N.V., pursuant to Master Gaming License #8048/JAZ issued by the Governor of Curaçao.

iMoon is committed to maintaining the highest standards of integrity and compliance within the iGaming industry. Our Anti-Money Laundering (AML) Policy is designed to prevent and detect any misuse of our gaming products for the purposes of money laundering or the financing of terrorism. The policy applies to all iMoon games, platforms, and services, and outlines procedures for risk assessment, customer due diligence, monitoring, and reporting suspicious activity. This AML framework ensures that iMoon operates in full compliance with applicable international laws and regulatory requirements across all jurisdictions in which we offer our games.

2. Purpose

The purpose of iMoon's AML Policy is to establish a comprehensive framework that safeguards our operations against the risks of money laundering and terrorist financing. This policy is intended to ensure that iMoon identifies, assesses, and mitigates potential AML risks associated with the use of our gaming products. It serves to protect the integrity of our business, comply with all applicable regulatory obligations, and contribute to the broader global effort to combat financial crime. Through clearly defined procedures and ongoing staff awareness, the policy promotes a culture of compliance and accountability across all levels of the organization.

3. Audience

The AML Policy applies to a broad range of internal and external stakeholders involved in iMoon's operations. These include:

3.1 All Employees:

All staff, regardless of role or seniority, are responsible for understanding and adhering to the AML Policy and for reporting any suspicious activity.

3.2 Executive Management:

Responsible for enforcing the policy, providing resources for AML compliance, and setting the tone for a strong compliance culture.

3.3 Account Managers & Sales Teams:

Required to conduct enhanced due diligence on partners and operators and ensure client relationships are AML-compliant.

3.4 Subcontractors and Consultants:

Any third parties contracted to perform services on behalf of iMoon must comply with the principles of this policy.

3.5 Operators and Aggregators:

iMoon's B2B partners must demonstrate their own AML measures and cooperate fully with our compliance checks.

3.6 Third-party Suppliers and Service Providers:

Entities providing technical, financial, or operational services must support iMoon's efforts to identify and prevent illicit financial activities.

4. Definitions

Capitalized terms are defined in the relevant clauses.

5. Policy Implementation & Responsibilities

The implementation of iMoon's Anti-Money Laundering (AML) Policy is critical to ensuring compliance with applicable laws, protecting the integrity of our games, and maintaining trust with our partners. The following outlines how the policy will be executed:

- **Head of Legal – Policy Oversight and Maintenance**
The Head of Legal holds primary responsibility for maintaining, updating, and overseeing the enforcement of the AML Policy. This includes ensuring that the policy reflects current regulatory requirements, coordinating audits, and reporting to executive management on AML compliance.
- **Employee Awareness and Training**
All employees will receive AML training appropriate to their roles. This includes onboarding sessions and periodic refreshers to ensure awareness of red flags, reporting protocols, and regulatory obligations.
- **Customer and Partner Due Diligence**
Prior to engaging with operators, aggregators, or third-party suppliers, thorough Know Your Customer (KYC) and Customer Due Diligence (CDD) checks will be conducted. Ongoing monitoring will be carried out for high-risk entities.
- **Transaction Monitoring and Record-Keeping**
Systems will be in place to monitor unusual activity across our platform. Suspicious transactions will be flagged for further investigation. Detailed records will be securely maintained in line with legal retention requirements.
- **Internal Reporting Procedures**
Employees and stakeholders are required to promptly report any suspected instances of money laundering or financial misconduct to the Head of Legal or designated AML Compliance Officer. A clear, confidential reporting mechanism will be available.
- **Review and Audit**
The AML Policy and its enforcement processes will be reviewed at least annually, or more frequently if required by regulatory changes or internal risk assessments.

6. Business Risk Assessment

iMoon conducts a comprehensive Business Risk Assessment (BRA) to identify, evaluate, and mitigate the risks associated with money laundering (ML), terrorist financing (TF), and the financing of proliferation. This risk assessment is integral to ensuring that our policies, controls, and procedures are appropriate and proportionate to the nature and scale of our operations in the iGaming industry.

6.1. Risk Identification

The BRA examines the inherent risks associated with the following areas:

- **Products and Services:**
Analysis of how iMoon's fast-paced games (e.g., crash games, mines, and casino titles) could be misused for ML/TF purposes due to rapid transactional turnover, ease of access, and volume of players.
- **Customer Base:**
Identification of risk levels based on customer profiles, including jurisdiction, behavior, and source of funds. High-risk factors include anonymity, use of third-party accounts, and jurisdictions with weak AML frameworks.
- **Geographical Exposure:**
Assessment of risks associated with operating in or serving customers from high-risk jurisdictions identified by FATF or national authorities.
- **Delivery Channels:**
Consideration of the risks introduced through third-party operators, aggregators, or affiliates who may have varying levels of AML compliance.
- **Payment Methods:**
Review of the vulnerabilities associated with various payment channels, including prepaid cards, cryptocurrencies, and e-wallets.

6.2. Risk Evaluation

Each identified risk is evaluated in terms of:

- Likelihood of occurrence
- Potential impact on the business
- Effectiveness of existing controls

Risks are categorized as Low, Medium, or High to facilitate prioritization.

6.3. Controls and Mitigation

iMoon ensures that the following measures are in place to mitigate identified risks:

- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)
- Transaction monitoring tools with automated red flag detection
- Ongoing training for relevant staff
- Regular audits and reviews of compliance procedures
- Segmentation of customer profiles and limits based on risk levels

6.4. Ongoing Monitoring and Review

The BRA is reviewed at least annually or in response to significant changes in business operations, product offerings, or regulatory developments. The Head of Legal and Compliance is responsible for ensuring the risk assessment remains current and effective.

7. Customer Risk Assessment

As part of iMoon's Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) framework, a **Customer Risk Assessment (CRA)** is conducted for each player at the time of establishing a business relationship. This assessment determines the individual risk profile of the player and informs the level of due diligence and monitoring required throughout the relationship.

6.1. Purpose of the CRA

The primary purpose of the CRA is to evaluate the risk that a particular customer may use iMoon's services to engage in money laundering, terrorist financing, or other financial crimes. By assessing customer-specific risk factors, iMoon ensures proportionate and risk-based application of its AML controls.

6.2. Timing of the CRA

The CRA must be conducted:

- **During account registration**, prior to any transactional activity.
- **Prior to the establishment of a business relationship**, i.e., before granting full access to deposit, wager, or withdraw funds.
- **Periodically reviewed**, particularly when customer behavior changes significantly or new risks emerge.

6.3. Information Collected for Risk Profiling

To assess a customer's risk profile, iMoon collects and evaluates the following data:

- **Identity Information:**
 - Full name, date of birth, nationality
 - Proof of identification (e.g., passport, ID card)
 - Verification of identity through reliable, independent sources
- **Geographical Risk:**
 - Country of residence and IP location
 - Whether the customer is from a **high-risk jurisdiction** (as identified by FATF or EU)
 - Country's AML/CTF regulatory environment
- **Source of Funds / Wealth:**
 - Information on employment or income source
 - Declaration or documentation when required (e.g., for high deposit thresholds)
 - Use of third-party payment methods or crypto wallets
- **Behavioral Risk:**
 - Speed and frequency of deposits and withdrawals
 - Unusual betting patterns or gameplay behavior
 - Abrupt changes in transactional activity
- **Player Type and Channel Risk:**
 - Whether the player is self-registered or referred by a third-party
 - Use of VPN or other anonymization tools
 - Communication preferences and ability
- **Politically Exposed Person (PEP) & Sanctions Screening:**
 - Checks against global PEP, sanctions, and adverse media databases

6.4. Risk Classification Levels

Based on the information collected, players are assigned a **risk level**:

- **Low Risk:**
Verified identity and source of funds, from low-risk jurisdiction, consistent activity.
- **Medium Risk:**
Some risk indicators present (e.g., mid-risk jurisdiction, occasional unusual activity).

- **High Risk:** High-risk jurisdiction, large volume transactions, unclear source of funds, or flagged as PEP.

6.5. Risk-Based Actions and Monitoring

The customer's risk level determines the depth of due diligence and ongoing monitoring:

- **Low Risk:** Standard CDD, regular transaction reviews.
- **Medium Risk:** Enhanced transaction monitoring and periodic documentation checks.
- **High Risk:** Enhanced Due Diligence (EDD), approval from senior management, and continuous monitoring.

6.6. Review and Update

- Risk profiles are reviewed periodically or upon material changes in the customer's behavior, information, or regulatory status.
- The CRA is updated accordingly to ensure ongoing accuracy and compliance.

8. Contact Information

- 8.1 iMoon Support can be contacted at support@imoon.com.
- 8.2 iMoon's AML Policy may be found at imoon.com and imoon.casino.

9. AML, CFT and CDD Policy

- 9.1. As part of its global operations, iMoon has established compliance measures in-line with its products and services that are reasonably designed to deter and detect illicit activity on its platform(s). Such measures include onboarding and compliance screenings of its Users and transaction action-based controls.
- 9.2. In using the Website, the User agrees to be bound by the terms of this Anti-Money Laundering, Anti-Terrorism Financing and Due Diligence Policy. If a User does not agree with any part of this Policy, the User must not use or continue to use any iMoon website(s).
- 9.3. iMoon reserves the right to amend this Policy at any time and without advance notice. In the case of any amendments to this Agreement, iMoon is not required to, but will endeavor to take steps to bring such amendments/changes to a User's attention (such as for example via email or placing a notice on a Website). If a User continues using iMoon services after any amendment, such action will be deemed as the User's acceptance of the amendment and will be bound by the changes, updates and/or modifications in the amendment whether or not a User has been notified, seen or read the amendment(s).
- 9.4. The User must thoroughly read and understand these before creating an account and before using the Website. If a User decides not to read it, the User is still bound by this Agreement. If a User does not agree with any part of this Policy, a User must not use or continue to use any iMoon website.
- 9.5. All references to "Player" or "User" refers to any person who plays or uses iMoon's products services.
- 9.6. "Account" or "the Accounts" refers to any account created on iMoon website.
- 9.7. "AML/CFT" refers to Anti-Money Laundering and Combating the Financing of Terrorism.
- 9.8. "AMLCO" refers to Anti-Money Laundering Compliance Officer.

9.9. "CDD" refers to Customer Due Diligence.

9.10. "Curaçao Gaming Control Board" refers to the regulator for the Curaçao casino industry.

9.11. "FATF" refers to Financial Action Task Force.

9.12. "KYC" refers to Know Your Customer.

9.13. "Third-party" or "Third-party Partner" refers to a business other than an iMoon entity.

10. iMoon AML/CFT Statement

10.1. iMoon is not a financial institution within the meaning of applicable law of Curaçao and also it is not directly subject to the statutes and regulations applicable to financial institutions, money transfer or virtual asset service providers. However, in accordance with the 2016 Regulation for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), which is applicable for the Curaçao jurisdiction, as provided by the Curaçao Gaming Control Board, iMoon expressly prohibits and rejects the use of iMoon products for any illicit activity, including but not limited to money laundering, terrorist financing or trade sanctions violations, consistent with various national anti-money laundering laws, regulations and norms.

10.2. iMoon continues to monitor and abide by the parameters promulgated by the Financial Action Task Force (FATF) and gaming trade groups, in addition to the Curaçao Gaming Control Board and will take necessary action, as it deems appropriate, to reflect changes in law.

10.3. iMoon's intention is to follow the global best practices in guarding against iMoon products being used to facilitate activities stated in 3.1 above. iMoon's best practices include:

- The adoption of a written policy and procedures and controls, reasonably designed to guard against money laundering, terrorist financing and trade sanctions violations.
- A designation of a compliance officer to oversee the implementation of this policy, where appropriate.
- A provision of related education and training to relevant employees; and
- Independent reviews, monitoring and maintenance of this policy.

11. Know your Customer (KYC) and Customer Due Diligence (CDD)

11.1. iMoon applies appropriate ongoing monitoring measures. iMoon uses a combination of its software development, internal operational features and other services to ensure that it complies with the law.

11.2. iMoon has adopted a risk-based Customer Due Diligence (CDD) to understand the nature and purpose of the relationship between a User and the iMoon platform in order to develop a customer risk profile. To implement it, iMoon collects certain documentary and non-documentary information at account-opening corresponding with the nature of the account and services that iMoon offers. iMoon maintains different CDD for other accounts and services.

11.3. The CDD consists of:

- 11.3.1. Collecting baseline information (e.g., address, email address) at account creation on iMoon's User

portal;

11.3.2. Monitoring the risk profile associated with an underlying currency account used to fund the User's account;

11.3.3. Maintaining records of the information used to identify a User; and

11.3.4. Determining if a User appears on any list of known or suspected terrorists or terrorist organizations based on the above information.

11.4. The above steps are implemented using the following measures:

- **Identity and Age Verification:** A third-party service provider supports iMoon's ability to determine the legitimacy of the identification and KYC materials or information provided and will ensure that the User is allowed to create an account on iMoon. The service provider also confirms that the User does not appear to be in a sanctioned or prohibited jurisdiction and will search global sanctions lists to verify that a User does not appear using onboarding information such as addresses.
- **Customer Information:** iMoon collects details about each User to form a reasonable belief that iMoon knows the identity of its Users according to the User's risk profile. For example, iMoon may collect KYC details, including but not limited to name, address, country, date of birth and postal code. The above KYC Information will be collected prior to issuing an iMoon funding address to Users. iMoon does not allow Users who are non-natural persons.
- **Geo-blocking for Prohibited Jurisdictions:** iMoon requires contractual client certifications. No gaming services will be offered to IP address based in geo-blocked countries, where such activity is not permitted.
- **Geo-blocking for Sanctioned Jurisdictions:** iMoon requires Users to certify that a User is not subject to sanctions or watch lists, associated with sanctioned jurisdictions. iMoon relies on various risk-based measures to verify these representations and through IP address-based geo-blocking.
- **Contractual Prohibitions on Users Onboarding from Prohibited Jurisdictions:** Users are notified at onboarding that iMoon does not offer services in restricted jurisdictions. iMoon's policy restricts the User activity in countries from a combination of risk, fraud prevention and AML standards, as well as any assessments associated with the permissibility of its services in certain jurisdictions.

11.5. Ongoing Monitoring. iMoon performs ongoing monitoring of its Users to detect any behaviors or indicators that might raise suspicions regarding money laundering and terrorism financing practices. For that purpose, iMoon implements a set of red flag indicators to help determine such behaviors and may require further action from iMoon in assessing the User information.

11.6. **Due Diligence (DD).** Whenever one of those red flags is triggered, a User's account will be suspended and iMoon will pursue enhanced due diligence. KYC diligence under this policy is deemed to include, but not limited to, the provision of:

11.6.1. Full legal name;

11.6.2. Country of citizenship;

11.6.3. Permanent address (for an individual, it must be a residential or business address, and for an entity, it must be a principal place of business, local office or other physical location);

11.6.4. Identification number (either a taxpayer identification number or, if unavailable, a passport number and country of issuance, alien identification card number or number and country of issuance of another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard);

11.6.5. Identification documents; and

11.6.6. Source of funds and source of wealth.

11.7. **Third Party DD.** iMoon may use a third-party service provider to verify any of the above information to establish a reasonable basis to know the User's true identity where the User's activity warrants such action.

11.8. iMoon will not accept and will block Users that:

- Do not provide the identification information requested by iMoon;
- If it is determined, fake identification documents were provided;
- User who tries to deceive their location;
- Are from restricted or prohibited jurisdictions;
- Are subjected to sanctioned jurisdictions or watch lists;
- Are gambling addicted or have mental health issues;
- The source of funds originated or exchanges in restricted jurisdictions.

11.9. Social media cross-check

11.9.1. iMoon may ask the User to connect to Facebook or Instagram account with the User's iMoon account to support KYC verifications and checks.

11.9.2. If the User chooses to connect on Facebook or Instagram account with their User's iMoon account, iMoon gets access to User's information, posts, pictures and location data connected to their Facebook/Instagram account.

11.9.3. The system will use the User's Facebook or Instagram account to cross-check all information given in the KYC check for accuracy and completeness. iMoon and its third-party partners will not post anything from the User's account or affect the Facebook or Instagram account in any visible way.

12. Transactions Monitoring & Compliance

12.1. iMoon is committed to complying with economic and trade sanction programs. For that purpose, iMoon established a transaction monitoring program with controls and processes to identify and detect any unusual activity in real-time.

12.2. **Reporting.** iMoon conducts ongoing monitoring on a regular basis using rule-based systems developed in-house and others from third-party vendors to review a User's history and patterns of activity to detect and report any unusual activity as required and to create and implement any additional controls or limits on its platform.

12.3. iMoon may, in its reasonable discretion, impose certain due diligence requests on a User balance withdrawal. iMoon conducts a mixture of manual and automated transaction monitoring processes to identify suspicious behavior. Where such behavior is identified, iMoon may refuse to process any withdrawal attempts or collect additional information from the recipient. iMoon further endeavors to limit a User's attempt to fund from prohibited jurisdictions, wherein the associated address indicates that the

User or the User's funds are located in a prohibited jurisdiction.

- 12.4. Prior to issuing an iMoon address to a User, iMoon screens a User's address against applicable sanction databases. Such screening measures rely on third-party blockchain forensics vendors. (iMoon will periodically re-screen addresses against such databases.)
- 12.5. iMoon monitors account activity for unusual size, volume, pattern or type of transactions, considering risk factors and red flags appropriate to its business. Monitoring is conducted by running regular reports of unusual, high-risk or suspicious User activity.
- 12.6. iMoon uses software designed to detect suspicious deposits and withdrawal patterns. Such instances are dealt with on a case-by-case basis, depending on the perceived level of risk. In such cases, a User may be required to explain their methodology and purpose for using the platform.
- 12.7. Deposits and withdrawals, both indirect and direct, are reviewed for signs of fraud and general suspicious behavior. If an alert of potential illicit behavior is triggered, a User's account is suspended and inspected. Sufficient proof of wealth may be requested from high-risk accounts. iMoon may refuse to withdraw to certain "high-risk" addresses.
- 12.8. Once an account reaches its withdrawal limit based on the accounts risk characterization over the life of the account, each account is assessed for another round of KYC if suspicious activity is determined.
- 12.9. iMoon uses third-party service providers to assist in software designed to detect the use of multiple accounts by one User. This software relies on detecting links between the same devices used to access various accounts. Such instances are dealt with a case-by-case basis, depending on the perceived level of risk.
- 12.10. iMoon monitors a User activity within the iMoon platform and any withdrawal must meet iMoon's and its third-party service provider's verification processes. iMoon further prohibits peer-to-peer account transfers within the iMoon platform infrastructure. Any attempts to circumvent this restriction will be treated as an abuse.
- 12.11. iMoon has implemented time zone controls that detect a User's device information and crosses it with restricted jurisdictions to understand if a User is trying to use geo-location software to hide the jurisdictions from which they are connecting.
- 12.12. iMoon works with reputable third-party service providers as part of its compliance infrastructure. iMoon periodically assesses the strength of its key third-party service providers to determine if additional services are needed, that is, if a third-party service provider is not performing consistently with its contractual obligations, or if another remedial action is necessary for iMoon to comply with this policy. iMoon may request information from a third-party service provider as part of its vendor review process.
- 12.13. iMoon continuously monitors for any non-documentary compliance, testing or trial programs on a limited basis with such compliance vendors to determine the effectiveness of such programs. Blockchain native compliance tools include fraud prevention services, on-chain KYC providers, and other tools designed to reflect the technological features associated with blockchain platforms.

13. Education and Training

- 13.1. iMoon, with the assistance of its legal counsel and under the oversight of its management, provides employees with AML, anti-terrorist financing and trade sanctions compliance training, as deemed appropriate.

14. Reporting

- 14.1. iMoon is obliged to report any unusual or suspicious transactions, such as Users that are identified as being on a sanctions list, links to money laundering, terrorism financing or other criminal activities are reported as a suspicious activity to regulators. iMoon aims to fully cooperate with authorities in the shared fight against illicit and illegal activities.

15. Failure to Comply with AML Policy

Non-compliance with iMoon's Anti-Money Laundering (AML) Policy can expose the company, its employees, and affiliated partners to serious **legal, regulatory, financial, and reputational risks**. All stakeholders—including employees, subcontractors, operators, and third-party suppliers—must strictly adhere to this policy and related procedures.

15.1. Legal and Regulatory Consequences

- **Regulatory Sanctions:** iMoon may be subject to fines, penalties, license suspension or revocation by gaming authorities such as the MGA or other national regulators if found in breach of AML requirements.
- **Criminal Liability:** Willful or negligent involvement in money laundering or terrorist financing activities can result in criminal charges for both the company and individuals involved, including imprisonment, fines, and permanent disqualification from working in regulated industries.
- **Contractual Breaches:** Violation of AML obligations may result in the termination of contracts with operators, partners, and B2B aggregators.

15.2. Business Risks

- **Loss of License:** iMoon's failure to implement effective AML controls may lead to revocation or non-renewal of gaming licenses across jurisdictions.
- **Loss of Partners and Clients:** Reputational damage may erode trust with key partners, operators, and clients, leading to terminated business relationships.
- **Increased Oversight and Audits:** Regulatory bodies may impose intensified supervision, unannounced audits, or impose additional reporting obligations.

15.3. Disciplinary Actions

Violations by employees or internal staff will result in disciplinary measures, including:

- Formal warning
- Temporary suspension
- Demotion or reassignment
- Termination of employment
- Reporting to relevant authorities where appropriate

15.4. Reputational Damage

- Public association with AML breaches or investigations can severely damage iMoon's brand reputation, trustworthiness, and credibility in the international iGaming industry.

16. Miscellaneous

- 16.1. Every User acknowledges that iMoon is the final decision-maker on whether or not the User has violated iMoon rules, policies and terms of use in a manner that results in suspension or permanent barring from participation on iMoon website(s).
- 16.2. **Policy History.** This AML Policy supersedes and replaces all previous anti-money laundering policies, procedures, and guidelines previously issued by iMoon. It serves as the current and sole authoritative framework for the prevention of money laundering, terrorist financing, and proliferation financing within the organization. All stakeholders are required to comply with this version of the policy going forward.
- 16.3. iMoon's Terms of Use apply.



20.05.2025.