

Anti-Money Laundering (AML) Program and Compliance Procedures

1. Company Policy

1.1 It is the policy of RSP Entertainment N.V (the "Company") to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company strives to comply with all applicable requirements under the legislations in force in the jurisdictions in which the Company operates, to prevent the use of the financial system for the purpose of money laundering and terrorist financing.

1.2 The Company is licensed and regulated by Curaçao Gaming Authority to offer games of chance under license number OGL/2024/168/0127 in accordance with the National Ordinance on Games of Chance (Landsverordening op de kansspelen, P.B. 2024, no. 157). The Company is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

2. Objective of the Policy

2.1 The Company is fully committed to be constantly vigilant to prevent money laundering and combat the financing of terrorism to minimize and manage risks such as the risks to its reputation risk, legal risk, and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes.

2.2 The Company will endeavor to keep itself updated with developments both at the national and international level on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, always, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorist and other criminal activities.

2.3 The Company's policies, procedures, and internal controls are designed to ensure compliance with all applicable laws, rules, directives, and regulations relevant to the Company's operations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures, and internal controls are in place.

3. Business and Customer Risk Assessments

The Company adopts a Risk-Based Approach (RBA) in accordance with GCB regulations. This involves:

3.1 Business Risk Assessment (BRA)

- Identifies inherent risks associated with the Company's services, jurisdictions, player types, and products

- Considers risk factors including: customer profile, transaction behavior, payment methods, delivery channels, and geographic exposure
- Includes results from the Curaçao National Risk Assessment (NRA)
- Reviewed annually or upon any operational or regulatory changes
- The BRA is formally approved by the Board of Directors and is reassessed at least annually or immediately following operational or regulatory changes. The methodology, data sources, risk categories, and rationale must be documented.

3.2 Customer Risk Assessment (CRA)

- Conducted during account registration or upon reaching the NAf. 4,000 threshold
- Players are categorized as Low, Medium, or High risk based on factors such as:
 - Source of funds
 - Geographic origin
 - Use of prepaid methods or anonymity tools
 - Volume and frequency of transactions
- CRA outcomes determine the applicable level of due diligence

3.3 Customer Acceptance Policy (CAP)

The Company maintains a Customer Acceptance Policy which outlines:

- Player types considered high risk, such as:
 - Politically Exposed Persons (PEPs)
 - Players with complex transaction patterns
 - Players from high-risk jurisdictions or sanctioned countries
- When to decline or terminate relationships, including:
 - Refusal to provide verification documents
 - Use of third parties to deposit/withdraw funds
 - Level of due diligence applicable to each risk category
- Sanctions screening and PEP identification performed at onboarding and regularly during the relationship

4. Player Identification Program

4.1 The Company will take reasonable steps to establish the identity of any person for whom it is proposed to provide its service (hereinafter "Players"). For this purpose, the process for the

registration of Players provided for under the General Terms and Conditions of the Company provides for the due diligence process that must be carried out before the opening of a user account.

4.2 The Company will always keep a secure online list of all registered Players and information, and documents will be retained in accordance with the applicable data protection obligations.

4.3 The Company will collect certain minimum Player identification information from each Player who opens an account. The Company will not accept to open anonymous accounts or accounts in fictitious names such that the true beneficial owner is not known.

4.4 Upon registration, players must provide full name, date of birth, nationality, place of birth, residential address, valid email, and username. This information will undergo screening against UN, EU, and local sanctions lists, as well as checks for Politically Exposed Persons (PEPs) via NameScan.

4.5 Documents to verify the identity information received will be requested from the Player when there is a risk or uncertainty about the information provided and is mandatory when the player engages in financial transactions equal to or exceeding NAf. 4,000 (approx. EUR 2,000), including single or linked transactions. Verification must be completed before any further deposits or withdrawals may occur. No additional funds may be deposited or withdrawn until identity verification is complete. If the threshold is hit through a withdrawal request, the account must be frozen until CDD is completed.

These documents shall include, to the extent permitted under the relevant data protection regulations:

- A copy of a valid identity card or passport
- Proof of address

4.6 The Company may supplement the use of documentary evidence by using other means, which may include:

- Independently verifying the Player's identity through the comparison of information provided by the Player with information obtained from a reporting agency, public database, or other source.
- Checking references with financial institutions; or
- Obtaining a financial statement

4.7 The Company will inform relevant Players that the Company may seek identification information to verify their identity.

4.8 Any employee of the Company who becomes aware of an uncertainty in relation to the accuracy and truthfulness of the Player information provided shall immediately notify the AML Compliance Person, who will review the materials and determine whether further identification is required and or so that it may be determined whether a report is to be sent to the relevant authorities.

4.9 If a potential or existing Player either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, the AML Compliance Person will be notified so that it may be determined whether a report is to be sent to the relevant authorities.

4.10 If there is suspicion or evidence that a Player is acting on behalf of another, beneficial ownership checks must be conducted. This includes determining if other parties hold more than 25% control or ownership.

4.11 If a Player has been identified as attempting or participating in any criminal or unlawful activity, the Company will take the appropriate steps to immediately freeze the account of the Player.

4.12 If any material personal information of a Player changes, verification documents will be requested.

- Additionally, the Company will track identity document expiry dates and request renewed verification when documents near expiration. Periodic reassessment of identity data will be conducted on a risk-sensitive basis and whenever material changes (e.g., address, payment method) are observed

5. Continuous Transaction Due Diligence

5.1 The Company will monitor account activity with special attention, and to the extent possible, the background and purpose of any more complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.

5.2 Monitoring will be conducted through the following methods: Transactions will be automatically monitored and reviewed daily for all transactions above 1000 EURO along with all the details of the users making those transactions. This includes comparing activity to the player's profile (expected income, geographic risk, behavior). Patterns that do not match the profile must trigger EDD and may require source of funds verification. Documents may be required at the determination of the AML Compliance Person.

5.3 The AML Compliance Person will be responsible for this monitoring, will review any activity that the monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the relevant authorities.

5.4 SDD is only applicable for low-risk customers using transparent financial methods.

It cannot be used if:

- There's any suspicion of money laundering or terrorism financing
- The player is a PEP or from a high-risk jurisdiction

5.5 EDD must be applied when a customer is from a high-risk jurisdiction, is a PEP, uses anonymity-favoring tools (e.g. prepaid cards), or when large or unusual transactions occur.

- In high-risk cases, the Company will collect a detailed statement on the player's source of funds (SoF) and source of wealth (SoW). This will include, where relevant: employer, salary range, business ownership, asset details. Supporting documentation such as payslips, tax returns, or bank statements may be requested depending on the risk severity.

EDD applies in all high-risk situations and includes:

- Collecting detailed source of funds and source of wealth
- Senior management approval before account continuation
- More frequent identity and transaction reviews
- Regular PEP and sanction re-screening, within 30 days of change detection

5.6 Parameters that signal possible money laundering or terrorist financing include, but are not limited to:

- Wire transfers to/from financial secrecy havens or high-risk geographic locations without an apparent reason
- Many small, incoming wire transfers or deposits made using checks and money orders
- Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent specific purpose

5.7 When an employee of the Company detects any activity that may be suspicious, he or she will notify the AML Compliance Person. AML Compliance Person will determine whether and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report.

5.8 The Company will not accept cash or non-electronic payments from Players. Funds may be received from Players only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer cheques, and any other method approved by the Company or respective regulators.

5.9 The Company will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.

5.10 To the extent the Company utilizes a third party to process and record payments to and from Player and accounts, the Company will use best efforts to ensure the service provider has transaction monitoring systems in place which will allow for screening of the transactions pursuant to these provisions and in accordance with the applicable legislation. The AML

Compliance Person shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

5.11 Records relating to the financial transactions shall be maintained in accordance with the data protection and retention requirements in the applicable jurisdiction of Curaçao.

6. Suspicious Transactions and Reporting

The AML Compliance Person will report any suspicious transactions (including deposits and transfers) conducted or attempted by, at or through a Player account involving EUR 1,000 or more of funds (either individually or in the aggregate) where the AML Compliance Person knows, suspects or has reason to suspect:

6.1 The Player is included on any list of individuals assumed associated with terrorism or on a sanction list.

6.2 The transaction involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations or to avoid any transaction reporting requirement under law or regulation.

6.3 The transaction has no ordinary lawful purpose or is not the sort in which the Player would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction.

6.4 The transaction involves the use of the Company to facilitate criminal activity.

7. Training Programs

7.1 The Company will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. The training will occur on at least an annual basis. It will be based on the Company's size, its Player base, and its resources and be updated as necessary to reflect any new developments in the law.

7.2 Annual AML/CFT training is required for all employees and a record of completion must be kept. Training includes Curaçao AML obligations, escalation paths, use of tools, and non-compliance consequences.

7.3 The training will include, at a minimum:

- New Employees: Intro to AML laws, red flags, and reporting obligations
- Customer-facing Staff: Recognizing suspicious patterns, verifying identity
- Audit Team: Updates on regulation, transaction testing, red flag evaluation
- Compliance Staff: Advanced AML trends, legal updates, and reporting standards
- Management: Governance responsibilities and reputational risks
- Training must be documented by name, date, scope, and test results

8. Compliance with AML Regulations

8.1 Company takes sanctions compliance and anti-money laundering (AML) regulations very seriously. To ensure that we are operating in a responsible and legal manner, we have implemented the following policies:

- Use of NameScan AML Solution: We utilize NameScan AML solution for screening all players and transactions to identify any potential matches with individuals or entities on sanctions lists or watchlists
- By adhering to these policies and utilizing advanced screening tools like NameScan AML solution, we are committed to maintaining a safe and secure online gambling environment for all our players
- No business may be conducted with persons from UN/EU/OFAC sanctioned countries. Daily screening must be performed using updated sanctions lists. Frozen account processes must align with national decrees
- Ongoing Monitoring and Compliance: We continuously monitor sanctions lists and regulatory updates to ensure that our policies and procedures remain up-to-date and compliant with all relevant laws and regulations
- Reporting Suspicious Activity: If we identify any suspicious activity or transactions that may be indicative of money laundering or terrorist financing, we will promptly report such activity to the appropriate authorities and take appropriate action in accordance with our AML policies, including the Financial Intelligence Unit (FIU) and other regulatory bodies
- Any suspicious transaction equal to or exceeding NAF. 4,000 must be reported to the FIU through GoAML. Transactions must be evaluated for links to ML/TF, unusual patterns, or involvement with sanctioned entities
- Compliance with AML Regulations: We comply with the anti-money laundering regulations set forth by the Curacao Gaming Control Board (GCB) license. This includes conducting customer due diligence, monitoring transactions for suspicious activity, and reporting any suspicious transactions to the Financial Intelligence Unit (FIU) in Curacao
- Regular FIU Reports: We make regular reports to the Curacao regulatory body GoAML about our suspicious transaction monitoring activities. These reports help us to identify and prevent money laundering and terrorist financing activities within our online gambling platform

9. Independent AML Audit

The Company will subject its AML compliance program to independent testing at least annually. This audit will be conducted by qualified internal audit personnel or an external expert with AML certification. The audit scope will include:

- Compliance with CDD and UTR reporting standards

- Testing of the transaction monitoring systems
- Assessment of training program effectiveness
- Review of compliance records and employee interviews

10. Company Compliance Officer Duties

- Designing and maintaining the AML Program in line with Curaçao laws and CGA directives
- Verifying adherence to the National Ordinance and Ministerial Decrees
- Reviewing internally reported unusual transactions and preparing reports for the FIU
- Maintaining complete records of UTRs and blocked accounts
- Organizing annual AML training across departments
- Performing deeper investigations into suspicious activities when necessary
- Proposing updates to the AML program in line with international developments
- Ensuring account freezing decisions avoid tipping off the player

11. Compliance and Consequences of Non-Compliance

Continued diligence, staff training, and adaptation to evolving legal and tech landscapes are essential to maintaining compliance and safeguarding operations.

Business Risks of Non-Compliance:

a. Reputational Risk:

- Brand damage from ML/TF associations

b. Regulatory Risk:

- License revocation, payment network blacklisting

c. Operational Risk:

- Legal costs, system overhauls, audit failures

12. Related Laws, Regulations & Guidelines

12.1 Curaçao Legal and Regulatory Frameworks:

- National Ordinance on Identification when Rendering Services (NOIS) N.G. 2017, no. 92

Link: <https://www.gamingcontrolcuracao.org>

- National Ordinance on the Reporting of Unusual Transactions (NORUT) N.G. 2017, no. 99

Link: <https://www.gamingcontrolcuracao.org>

- Sanctions National Ordinance N.G. 2014, no. 55

- FIU Curaçao (GoAML Reporting Platform)

Link: <https://www.fiu-curacao.cw>

12.2 International Guidelines:

- Financial Action Task Force (FATF) Recommendations

Link: <https://www.fatf-gafi.org>

- Caribbean Financial Action Task Force (CFATF)

Link: <https://www.cfatf-gafic.org>

- United Nations & European Union Sanctions Lists:

UN Sanctions: <https://www.un.org/securitycouncil/sanctions/un-sc-consolidated-list>

- EU Sanctions Map: <https://www.sanctionsmap.eu/#/main>

Approving Official(s):

Vladimir Shushkovsky, UBO

"RSP Entertainment N.V" 3 Abraham Mendez Chumaceiro Boulevard, Curacao

Effective Date:

01/02/2025

Next Review Date:

01/02/2026

VJ TECH
GROUP

Contact Information:

For any questions regarding this policy, please contact:

Olga Gavril'yik compliance@vjtechgroup.com

"VJ Tech Group LTD" 82 georgiou griva digeni, office 101, Limassol, CY 3101