

JW ENTERTAINMENT B.V. AML POLICIES

1. Objectives

It is the policy of. To actively prevent the services of the firm from being used to facilitate financial crime, money laundering, and terrorist financing.

Strict compliance with all applicable regulations will also protect the senior management and staff of the firm, as individuals, from the risks of breaches of the law, regulations, and supervisory requirements and preserve the reputation of JW Entertainment B.V. against the damage that could be caused by being implicated in money laundering and terrorist financing activities.

To achieve these objectives, it is the policy of this firm that:

- Every staff member shall meet their obligations as appropriate to their role and responsibilities;
- Commercial considerations cannot take precedence over **JW ENTERTAINMENT B.V.** 's anti-money laundering commitment;
- The firm shall appoint a Money Laundering Reporting Officer/Nominated Officer ("MLRO") and a deputy to cover in their absence, and they shall be afforded every assistance and cooperation by all members of staff in carrying out their duties and responsibilities. The deputy will be the Director Chief Executive Officer (CEO).

All domains will strictly comply with all applicable AML/CFT rules and regulations with specific emphasis on:

- A culture of compliance to be adopted and promulgated throughout the firm towards the prevention of financial crime;
- A commitment to ensuring that customer's identities will be satisfactorily verified at required thresholds;
- A commitment to "knowing its customer" appropriately - both at acceptance and throughout the business relationship - through taking appropriate steps to verify the customer's identity and monitoring their use of **JW ENTERTAINMENT B.V.** services;
- A commitment to ensuring that staff are trained and made aware of the law and their obligations under it, to establishing procedures to implement these requirements, and
- Recognition of the importance of staff promptly reporting their suspicions internally;

The risk-based approach, which is consistent with FATF Recommendation 1, is at the heart of our policies, procedures, and controls. This approach means that we focus our resources on the areas of greatest risk.

Our policies, procedures, and internal controls are designed to ensure compliance with all applicable anti-money laundering and anti-terrorist financing regulations and regulatory guidelines and will be reviewed and updated regularly to ensure appropriate policies, procedures, and internal controls are in place to account for both changes in regulations and changes in our business.

2. Money Laundering and Terrorism Financing

Money Laundering means:

- a. The conversion or transfer of property, knowing that such property is derived from criminal activity or an act of participation in such activity, to conceal or disguise the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;
- b. The concealment or disguise of the true nature, source, location, disposition, movement, or rights concerning, or ownership of, property, knowing that such property is derived from criminal activity or an act of participation in such activity;
- c. The acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or an act of participation in such an activity;
- d. Participation in, association to commit, attempts to commit, and aiding, abetting, facilitating, and counseling the commission of any of the actions referred to in points (a), (b), and (c).

Money laundering shall be regarded as such even where the activities that generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.

Terrorism financing means the provision or collection of funds by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, to carry out any terrorist act.

3. Organization of the AML/CFT function

3.1. Senior Management

Senior Management is responsible for the overall compliance policy of **JW ENTERTAINMENT B.V.** and ensuring adequate resources are provided for the proper training of staff and the implementation of risk systems. This includes computer software to assist in oversight. Senior management will receive and consider the monthly compliance reports sent by the MLRO and authorize changes based on the recommendations if required.

Senior Management consists of the Board of Directors, the Executive Management Committee, and the MLRO.

3.2. The Nominated Officer/Money Laundering Reporting Officer

Responsible for receiving internal disclosures and making reports to the Gaming Control Board, Curacao. First point of contact for all compliance issues from staff. Prepares monthly reports for

consideration of senior management and conducts risk assessments of compliance systems. Undertakes regular random analysis of transactions, including assessment of documentary evidence provided by customers. Assists in making any necessary amendments to AML Policy in line with risk assessment. Ensures everyone is periodically informed of any changes in anti-money laundering or anti-terrorist financing legislation, policies, and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs. Review customer identification information to ensure that all the necessary information has been obtained. Establishes and implements the risk scoring matrix following regulatory guidance and for review and approval by Senior Management.

3.3.Staff

Responsible for knowing the AML Compliance Policy and understanding responsibilities. Ensure company procedures are adhered to and obtain all documentary evidence as outlined within the manual. Ensure that all suspicious and unusual activity is reported to the MLRO.

4. The Compliance Programme

4.1.The Money Laundering Reporting Officer (MLRO)

JW ENTERTAINMENT B.V. has appointed an MLRO with full responsibility for JW'S DOMAINS' anti-money laundering compliance.

The MLRO:

- Will monitor **JW ENTERTAINMENT B.V. TRADING's** AML/CFT policies and respond to any reasonable request made by law enforcement and/or the Gaming Control Board, Curacao.
- Has the authority to act independently in carrying out their responsibilities, which includes direct access to the Gaming Control Board, Curacao, and appropriate law enforcement agencies, so that any suspicious activity may be reported to the right quarter as soon as is practicable.
- Has the authority and the resources necessary to discharge their responsibilities effectively.
- Is from a senior level and has direct access to senior management and the board of directors.
- May choose to delegate certain duties to other employees, but wherever such a delegation is made, the MLRO retains ultimate responsibility for the implementation of the compliance regime.
- At least annually, the MLRO will issue a report (the MLRO Report) to the senior management of JW'S DOMAINS on the operation and effectiveness of the money laundering controls. This report will cover improvements, remedial programs, the outcome of any internal audit reviews of the AML/CFT processes, and other relevant items.

4.2.Compliance Policies and Procedures

JW ENTERTAINMENT B.V. has policies and procedures to assess the risks related to money laundering and terrorist financing. These policies and procedures are:

- Written and maintained by the MLRO under the supervision of senior management
- Approved by senior management
- Communicated, understood, and adhered to by everyone dealing with customers or their transactions, including those who work in the areas relating to customer identification, record keeping, and reportable transactions, who need enough information to process and complete a transaction properly as well as to ascertain the identity of customers and keep records as required.
- Policies and procedures that incorporate the reporting, record keeping, customer identification, risk assessment, and risk mitigation requirements applicable.

Although directors and senior officers may not be involved in day-to-day compliance, they need to understand the statutory duties placed upon them, their staff, and **JW ENTERTAINMENT B.V.**

The policy also includes procedures to mitigate ML/TF risks arising from technological innovations. Prior to the launch of new products, services, or technologies, JW ENTERTAINMENT B.V. will:

- Conduct a risk assessment identifying vulnerabilities.
- Document the assessment and any corresponding mitigation measures.
- Review and update AML policies accordingly.

4.3. The Risk-Based Approach

In money laundering and terrorist financing, a risk-based approach covers the following:

- The risk assessment of customer relationships and business activities;
- The risk mitigation to implement controls to handle identified risks;
- Keeping customer identification, beneficial ownership, and business relationship information up to date and
- The ongoing monitoring of business relationships and transactions.

Existing regulatory obligations, such as for customer identification, are a minimum baseline requirement. Where enhanced due diligence is appropriate, a principle of the risk-based approach is to focus resources where they are most needed to manage risks within our tolerance level.

All risk-based measures will be reviewed periodically and upon changes in product offerings, customer base, or regulatory environment. Documented assessments shall be available for inspection by the Gaming Control Board.

4.4. Risk Mitigation

Risk mitigation is implementing controls to limit the potential money laundering and terrorist financing risks identified in the risk assessment to stay within the risk tolerance level. When the risk assessment determines that the risk is high for money laundering or terrorist financing, then we will develop risk mitigation strategies and apply them.

In all situations, risk mitigation controls and measures include:

- Focussing on operations (products and services, customers and business relationships, geographic locations, and any other relevant factors) that are more vulnerable to abuse by money launderers and criminals;
- Informing senior management of compliance initiatives, identified compliance deficiencies, corrective action taken, and suspicious transaction reports filed;
- Providing for program continuity despite changes in management, employees, or structure;
- Focussing on meeting all regulatory record keeping and reporting requirements, recommendations for anti-money laundering and anti-terrorist financing compliance, and providing timely updates in response to changes in requirements;
- Enabling the timely identification of reportable transactions and ensuring accurate filing of required reports;
- Incorporating anti-money laundering and anti-terrorist financing compliance into job descriptions and performance evaluations of appropriate personnel; and
- Providing for adequate supervision and training of employees that handle currency transactions, complete reports, monitor for suspicious transactions, or engage in any other activity that forms part of the anti-money laundering and anti-terrorist financing program.
- Increasing awareness of high-risk situations within all business lines;
- Increasing the frequency of ongoing monitoring of transactions or business relationships;
- Escalating the approval of the establishment of an account or relationship even if not otherwise required to do so;
- Increasing the levels of ongoing controls and reviews of relationships;
- Requesting high-risk customers provide additional, documented information regarding controls they have implemented to safeguard their operations from abuse by money launderers and terrorists;
- Verifying the identity of customers by reference to reliable, independent source documents, data, or information;
- Preventing any transaction with a potential customer until identification and account opening information has been obtained;
- Implementing an appropriate process to approve all relationships identified as high-risk as part of the customer acceptance process or declining to do business with potential customers because they exceed **JW ENTERTAINMENT BV's** risk tolerance level;
- Implementing a process to exit from an existing high-risk relationship, which management sees as exceeding **JW ENTERTAINMENT BV's** risk tolerance level.

4.5. Risk Assessment

JW ENTERTAINMENT B.V. is required to analyze potential threats and vulnerabilities to money laundering and terrorist financing to which the business may be exposed in a risk assessment.

The risk assessment will document and consider the following:

- Products, services, and delivery channels
- Geographic locations and areas of operation
- Customers

The risk assessment may identify high-risk situations for which risk mitigation controls and monitoring may be required. The risk assessment is not static and will change over time.

When a customer is identified as high-risk, they are subject to more frequent ongoing monitoring and updating of customer identification information, as well as any other appropriate enhanced measures.

All domains detained by JW shall perform an initial risk assessment at the beginning of a new customer relationship and for existing customers on an ongoing basis.

Business Risk Assessment (BRA)

JW ENTERTAINMENT B.V. shall conduct a documented Business Risk Assessment at least annually, or whenever there are material changes in business activities, geographic operations, or regulatory frameworks. The BRA shall:

- Identify all inherent ML/TF risks linked to products, services, delivery channels, customer types, and jurisdictions.
- Incorporate findings from the National Risk Assessment (NRA) published by the GCB.
- Define the company's risk appetite and mitigation strategies.
- Be approved by the Board of Directors and made available to the Gaming Control Board upon request.

A record of the methodology, sources, rationale for risk classifications, and outcomes shall be retained.

4.5.1. Client and Business Risk

The Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) will be formally documented and reviewed annually. High-risk products, services, jurisdictions, and customer types will be reviewed quarterly to ensure ongoing relevance.

4.5.1.1. Products, Services, and Delivery Channels

JW ENTERTAINMENT B.V. will identify products and services or combinations of them that may pose an elevated risk of money laundering or terrorist financing. For example, products and services that support the movement and conversion of assets into, through, and out of the financial system pose a high risk. Certain services have also been identified by financial regulators, governmental authorities, or other credible sources as being potentially high risk for money laundering or terrorist financing.

- Wire transactions;
- Transactions involving third parties;
- Non-face-to-face business relationships.

4.5.1.2.Geographic Locations and Areas of Operation

Certain geographic locations potentially pose an elevated risk for money laundering and terrorist financing. These have been described by the FATF and by other resources such as Transparency International.

Clients from or identified as linked to these countries will be regarded as high-risk:

- Any country subject to sanctions, embargoes, or similar measures;
- Any country identified by credible sources as providing funding or support for terrorist activities or that has designated terrorist organizations operating within their country;
- Any country known to be a tax haven, source of narcotics, or other significant criminal activity;
- Any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement;
- Any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations or as having significant levels of corruption.

JW ENTERTAINMENT B.V. does not do business with or provide services to anyone in any country belonging to a list of select countries subject to comprehensive international sanctions.

4.5.1.3.Customer Relationships

The risk assessment requires to know your customers (“KYC”). This is not limited to identification or record keeping, but it is also about understanding the customers – including their activities, transaction patterns, and how they operate.

Examples of the factors that will be considered are:

- How long we have known the customer and had a business relationship;
- Customers wanting to carry out large transactions;
- Customers with regulatory or enforcement issues;
- Customers with multiple online complaints;
- Customers whose identification is difficult to verify;
- Customers who are politically exposed.

Each customer is risk-rated as either posing a low, medium, or high risk of money laundering and/or terrorist financing. The rating given at the beginning of the business relationship may be adjusted after the re-assessment and may change over time. The level of customer due diligence will vary depending on the risk rating of the customer at the beginning of the relationship and as it changes. For all high-risk players, enhanced due diligence is applied right away.

Customer Due Diligence (CDD) must be completed when transactions exceed NAF. 4,000 or a series of linked transactions meets this threshold. JW ENTERTAINMENT B.V. will:

- Immediately freeze accounts if CDD is not completed within 30 days of threshold breach.
- Block withdrawals above this threshold until full verification is done.

4.5.1.4. Politically Exposed Persons (PEP)

- a) For “know your customers” processes, PEP includes:
- Individuals holding prominent public positions (e.g., heads of state, ministers, senior government officials, etc.)
 - Family members and close associates of PEPs
 - Individuals holding positions of significant authority in international organizations
- b) To identify the PEPs, **JW Entertainment** has a robust process that includes:
- Customer Due Diligence (CDD): Implement CDD procedures to collect relevant information about customers, including their names, addresses, occupations, and any affiliations with public or international organizations.
 - Ongoing Monitoring: Continuously monitor existing customers for changes in their status that could indicate they have become PEPs.
 - Third-Party Screening Tools: Utilize reliable third-party screening tools to identify PEPs against global databases and watchlists.
- c) In the due diligence process, PEPs can undergo Enhanced Due Diligence, which involves revising:
- Source of Funds and Wealth: Conduct thorough investigations into the source of funds and wealth of PEPs to assess the legitimacy of their financial activities.
 - Ongoing Monitoring: Maintain heightened monitoring of PEP relationships, including regular reviews of transaction patterns and activities.
 - Senior Management Approval: Obtain approval from senior management for establishing or continuing business relationships with PEPs.
 - Documentation: Maintain detailed records of all EDD procedures and findings.
- d) **JW Entertainment** is also dedicated to risk assessment and mitigation. To keep up with the expected and analyzed risks for PEPs:
- Conduct regular risk assessments to evaluate the specific risks posed by PEP relationships.
 - Develop and implement risk mitigation strategies, such as:
 - Limiting Exposure: Consider limiting exposure to high-risk PEPs or declining to do business with them altogether.
 - Additional Controls: Implementing additional controls, such as enhanced transaction monitoring and reporting requirements.

- Diversification: Diversifying the customer base to reduce concentration risk.
- e) To ensure compliance, staff undergo regular training on PEP (Politically Exposed Person) identification, risk assessment, and AML (Anti-Money Laundering) regulations. They are encouraged to promote vigilance and report suspicious activities.
- f) Staff must maintain accurate records of all PEP-related activities, including identification, screening, Enhanced Due Diligence (EDD), and risk assessments, and report any suspicious activities or potential money laundering or terrorist financing risks to the relevant authorities.

4.5.2. Independent AML Audit Function

An independent audit of the AML program will be conducted at least annually to assess:

- Effectiveness of internal controls and procedures.
- Adherence to Curaçao AML regulations.
- Implementation of MLRO recommendations.

Audit findings will be presented to the Board of Directors and used to update AML strategies.

4.5.3. Regulatory Risk

Regulatory risk means not meeting our obligations under applicable legislation. Examples of breaches of regulatory obligations include:

- Customer identification not done properly;
- Failure to train staff adequately;
- Not having an anti-money laundering and anti-terrorist financing (AML/CFT) program;
- Failure to report suspicious transactions;
- Not having an MLRO;
- Failing to keep complete customer records.

5. Sanctions Compliance and Proliferation Financing

JW ENTERTAINMENT B.V. shall maintain procedures to:

- Regularly screen all customers and transactions against UN and EU sanctions lists and any locally published Curaçao lists.
- Freeze without delay any assets belonging to sanctioned individuals or entities and notify the FIU Curaçao immediately.

- Prevent transactions or relationships with individuals involved in the proliferation of weapons of mass destruction.
- Monitor sanction list updates published by the GCB.

6. Suspicious transactions reporting

6.1. Reporting unusual transactions

The Company is obliged to report without delay to the FIU any unusual transaction carried out or intended to be carried out to the FIU.

A report shall contain, as far as possible, the following information:

- a. The identity of the client;
- b. The nature and number of the client's identification document;
- c. The nature, time, and location of the transaction;
- d. The volume, destination, and origin of the values involved in the transaction;
- e. The circumstances based on which the transaction is considered unusual.

The Company is further obliged to pay special attention to all complex and unusually large transactions and all unusual patterns of transactions with no apparent economic or clear purpose.

The Company shall keep the data relating to the notification and shall record them in such a way that the data can be provided and the transaction in question can be reconstructed to respond without delay to requests for information from the competent supervisor.

The Company must be registered in the Financial Intelligence Unit (FIU) Curaçao.

Reporting of unusual transactions takes place electronically via the normal reporting portal (<http://mot.cw/Web/MOTWeb/MOTWeb.nsf/web/goaml%20the%20new%20portal%20for%20fiu%20curacao>), to which the service provider, after registration and validation of his registration by the Financial Intelligence Unit Curaçao, is granted access.

A transaction is reported via the normal Reporting Portal by filling in a web form, which consists of two parts:

1. Information about the reporting service provider and its designated reporting person.

This information remains the same for every report made by this person.

2. The actual transaction information, which is entered for each transaction, according to the choices made when completing the web form. The Financial Intelligence Unit Curaçao will indicate which fields are mandatory and must be filled in for submission. The information must be filled in per transaction report should be filled in, such as applicable indicator(s) and further transaction-specific details and any attachments.

The reporting portal is written in the English language.

Indicators of unusual transactions for casino and online sports betting

I. Objective indicators

A) A transaction reported to the police or judiciary:

A transaction reported to the police or judiciary in connection with money laundering or the financing of terrorism is reported to the police or judicial authorities.

B) A proposed transaction carried out by or on behalf of a natural person, legal person, group, or entity included in a list drawn up under the Sanctions Ordinance:

A proposed transaction conducted by or for the benefit of a person, legal person, group, or entity that appears on a list established under the Sanctions Ordinance.

C) A transaction valued at NAf 5000,00 (€ 2.404,05) or more, whether such transaction is in cash, by check or other payment instrument, or by electronic means or other non-physical means.

This includes, in any case:

1. A giro transaction worth NAf 5000,00 (€ 2.404,05) or more:
2. A giro transaction is a transfer from a bank account of the service provider to a local or international bank account at the request of a customer to the service provider.
3. The depositing or releasing of cash values held on a deposit of NAf 5000,00 (€ 2.404,05) or more.
4. The sale to a client of gaming tokens worth NAf 5000,00 (€ 2.404,05) or more.
5. Payment of prize money worth NAf 5000,00 (€ 2.404,05) or more.

II. Subjective indicators

Suspected money laundering transaction or terrorist financing:

A transaction where there is reason to believe that it may be related to money laundering or financing of terrorism.

In the case of a subjective indicator, the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, and any other circumstance that may be relevant) has reasonable indications to presume that a transaction is related to money laundering or terrorism financing.

6.2. Deadline for reporting

For objective indicators, all reporting entities should send their unusual transaction reports within 48 hours after the transaction has been executed or after there has been an intention for a transaction.

For subjective indicators, the period between the execution of the transaction (or the intention to execute a transaction) and the moment the compliance officer receives the report should not exceed 24 hours.

6. Anti-bribery and Whistleblowing

As an extension to the AML/CFT efforts, **JW ENTERTAINMENT B.V.** also employs Anti-Bribery and Whistleblowing Policies and Procedures. These are standalone documents that are available to all employees and are part of their onboarding package.

7. Employee Background Checks

JW ENTERTAINMENT B.V. is committed to establishing and maintaining procedures that enable it to be satisfied as to the integrity of all new staff members and, by extension, their likeliness to follow the domain policies and procedures. To meet this requirement, the Human Resources Department is responsible for undertaking all of the checks listed about new members of staff and for retaining the appropriate records:

- Obtain and confirm references, if required;
- Confirm their employment history and the qualifications they have;
- Request a recent police conduct certificate; and
- Request details of any regulatory action taken against them.

8. Policy Policy Review and Version Control

- **Effective Date:** May 2025
- **Next Review Date:** May 2026
- **Version:** 1.0
- **Approval Authority:** Senior Management and Board of Directors

All previous versions shall be archived. This policy will be reviewed annually or as necessary to reflect regulatory changes or business developments.