

SUPERSTARS ENTERTAINMENT AML POLICIES

1. Objectives

It is the policy of **SUPERSTARS ENTERTAINMENT B.V.** 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 **SUPERSTARS 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 **SUPERSTARS 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).

SUPERSTARS ENTERTAINMENT will strictly comply with all applicable AML/CFT rules and regulations with specific emphasis on the following:

- A culture of compliance to be adopted and promulgated throughout the firm towards the prevention of financial crime;
- A commitment to ensuring that customers' 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 **SUPERSTARS ENTERTAINMENT B.V.** services;
- A commitment to ensuring that staff are trained and made aware of the law and their obligations under it, and 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.

Terrorist 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 **SUPERSTARS 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

This role includes receiving internal disclosures and reporting them to the Gaming Control Board in Curacao. The person is the main contact for compliance issues from staff, preparing monthly reports for senior management and assessing compliance risks. They analyze transactions randomly and review customer documents. They assist in updating the Anti-Money Laundering

(AML) Policy based on risk assessments and ensure employees are informed of changes in anti-money laundering and anti-terrorist financing laws.

MLRO also verify that all required customer identification information is collected. Finally, they create a risk-scoring matrix per regulatory guidelines for senior management's review and approval

3.3. Staff

The staff is responsible for understanding the AML Compliance Policy and their specific responsibilities. They must ensure that company procedures are followed and gather all necessary documentation as outlined in the manual. Additionally, all suspicious and unusual activities must be reported to the Money Laundering Reporting Officer (MLRO).

4. The Compliance Programme

4.1. The Money Laundering Reporting Officer (MLRO)

SUPERSTARS ENTERTAINMENT B.V. has appointed an MLRO with full responsibility for **SUPERSTARS ENTERTAINMENT B.V.** and its domains anti-money laundering compliance.

The MLRO:

- The Money Laundering Reporting Officer (MLRO) will oversee the daily operations of **SUPERSTARS ENTERTAINMENT B.V.** and ensure compliance with AML/CFT policies. The MLRO will respond to requests from law enforcement and the Gaming Control Board of Curacao.
- The MLRO has the authority to act independently, with direct access to the Gaming Control Board and law enforcement to report suspicious activity promptly.
- The MLRO has the necessary authority and resources to fulfill their responsibilities effectively and operates at a senior level, having direct access to senior management and the board of directors.
- Although the MLRO may delegate some duties, they maintain ultimate responsibility for compliance.
- Annually, the MLRO will provide a report to senior management on the effectiveness of money laundering controls, including improvements and outcomes of internal audits.

4.2. Compliance Policies and Procedures

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

- The policy is written and maintained by the Money Laundering Reporting Officer (MLRO) under senior management's supervision and approval.

- It must be communicated to and understood by all employees interacting with customers, including those handling customer identification, record keeping, and reportable transactions, ensuring they have the information needed to complete transactions and verify identities.
- The policies should cover reporting, record keeping, customer identification, risk assessment, and risk mitigation.

Directors and senior officers must understand their statutory responsibilities, even if they do not manage day-to-day compliance.

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.

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:

- Focus on operations vulnerable to money laundering and criminal abuse, including products, services, customers, and geographic locations.
- Keep senior management informed about compliance initiatives, deficiencies, corrective actions, and suspicious transaction reports.
- Ensure program continuity amid changes in management, employees, or structure.
- Meet all regulatory record-keeping and reporting requirements and provide timely updates for compliance changes.
- Facilitate timely identification of reportable transactions and ensure accurate report filing.
- Integrate AML and ATF compliance into job descriptions and performance evaluations.
- Train and supervise employees involved in currency transactions and monitoring for suspicious activities.

- Increase awareness of high-risk situations and enhance monitoring of transactions and relationships.
- Escalate approvals for establishing accounts or relationships as needed.
- Request additional documentation from high-risk customers on their protective measures against laundering and terrorism.
- Verify customer identities using reliable documents and data.
- Delay transactions until identification and account opening information is obtained.
- Implement processes for approving or declining high-risk relationships based on **SUPERSTARS ENTERTAINMENT BV**'s risk tolerance.
- Create an exit strategy for existing high-risk relationships that exceed risk tolerance levels.

4.5. Risk Assessment

SUPERSTARS ENTERTAINMENT B.V. is required to and will 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 highlight high-risk situations that require risk mitigation controls and ongoing monitoring. It is important to note that the risk assessment is not static; it evolves over time.

When a customer is classified as high-risk, they will undergo more frequent monitoring and updates to their identification information, along with any other necessary enhanced measures.

Superstars Entertainment B.V. will conduct an initial risk assessment at the start of a new customer relationship and will continue to assess existing customers on an ongoing basis.

4.5.1. Client and Business Risk

4.5.1.1. Products, Services, and Delivery Channels

SUPERSTARS 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 associated with, the following countries will be considered high-risk:

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

SUPERSTARS 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 you 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 assigned a risk rating of low, medium, or high concerning money laundering and/or terrorist financing. This initial rating may be adjusted during periodic reassessments and can change over time. The level of customer due diligence conducted will differ based on the customer's risk rating at the start of the business relationship and as it evolves. For all high-risk customers, enhanced due diligence measures are implemented immediately.

Superstars Entertainment has procedures in place to verify identity by analyzing government-issued documents and confirming addresses to ensure that identity verification requirements are met. As the risk level changes, additional documents may be requested to validate the client's identity.

If suspicious activity is detected, further steps may be taken to verify the activity and reassess the client's risk level.

4.5.1.4. Politic Exposed Person (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, Superstars Entertainment has a robust process that includes the following:
 - 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) Superstars 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: Implement additional controls, such as enhanced transaction monitoring and reporting requirements.
 - Diversification: Diversifying the customer base to reduce concentration risk.
- e) To ensure compliance, staff undergoes 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. Regulatory risk

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

- Inadequate customer identification procedures.
- Insufficient staff training.
- Absence of an anti-money laundering and anti-terrorist financing (AML/CFT) program for the bot.
- Failure to report suspicious transactions.
- Lack of a Money Laundering Reporting Officer (MLRO).
- Incomplete customer record keeping.

5. Suspicious transactions reporting

5.1. 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 type 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 funds involved in the transaction.
- e) The circumstances that make the transaction unusual.

The Company must pay close attention to complex or large transactions and unusual patterns lacking an apparent economic purpose. It should be vigilant for signs of suspicious behavior, such as customers who hesitate to provide complete information, offer inconsistent details, or refuse identification. Background concerns may include criminal records or negative reports. Unusual behaviors like nervousness or excessive secrecy, as well as opening multiple accounts without clear reasons, are also warning signs.

Cash-related issues can arise from large cash transactions, frequent use of negotiable instruments, or cash deposits followed by wire transfers. Other red flags include unusually large or frequent transactions, sudden pattern changes, and dealings with high-risk countries.

Transactions involving round dollar amounts, those just below reporting thresholds, or rapid fund transfers require closer scrutiny. Additionally, complex transactions that obscure fund sources or payments to shell companies are concerning. The Company must keep records of all notifications to respond quickly to requests from supervisory authorities.-The Company must be registered in the Financial Intelligence Unit (FIU) Curaçao.

Unusual transactions are reported electronically through the standard reporting portal (<http://mot.cw/Web/MOTWeb/MOTWeb.nsf/web/goaml%20the%20new%20portal%20for%20fiu%20curacao>). Service providers who register and validate their registration with the Financial Intelligence Unit of Curaçao will gain access.

To submit a transaction, users must complete a web form divided into two sections:

1. Reporting Service Provider Information: Details about the service provider and designated reporting person, which remain the same for all reports.
2. Transaction Information: Specific details for each transaction, including mandatory fields specified by the Financial Intelligence Unit. Users must provide applicable indicators, transaction specifics, and any necessary attachments.

I. Objective indicators

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

- c. 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:
- d. 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.
- e. 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:

- a. A transaction worth NAf 5000,00 (€ 2.404,05) or more
- b. A 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.
- c. The depositing or releasing of cash values held on a deposit of NAf 5000,00 (€ 2.404,05) or more.
- d. The sale to a client of gaming tokens worth NAf 5000,00 (€ 2.404,05) or more.
- e. Payment of prize money worth NAf 5000,00 (€ 2.404,05) or more.

II. Subjective indicators

- a. A transaction may be flagged if there is reason to believe it could be linked to money laundering or the financing of terrorism.
- b. For subjective indicators, a transaction is deemed unusual if the reporting entity, using its understanding of its clients—including their income, business activities, and any other relevant circumstances—has reasonable grounds to suspect that the transaction is associated with money laundering or terrorism financing.

5.2. 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, **SUPERSTARS 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

SUPERSTARS ENTERTAINMENT B.V. is dedicated to establishing and maintaining procedures that ensure the integrity of all new staff members and their likelihood of adhering to the **Superstars Entertainment B.V.** policies and procedures. To fulfill this requirement, the Human Resources Department is responsible for conducting all necessary checks on new employees and maintaining appropriate records. These checks include:

- Obtaining and confirming references, if required.
- Verifying employment history and qualifications.
- Requesting recent police conduct certificate.
- Gathering information on any regulatory actions taken against them.