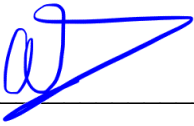


AML/CTF Policy

IN-AML-029-01

Signed by:

eMagnus Curacao B.V., Managing Director

A handwritten signature in blue ink, consisting of a stylized 'e' followed by a long horizontal stroke.

Date: 9/2/2025

A handwritten signature in blue ink, consisting of a stylized 'e' followed by a long horizontal stroke.

Table of Contents

1. Policy Statement.....	3
2. Purpose.....	3
3. Audience.....	3
4. Definitions.....	3
5. Policy Implementation.....	4
5.1. Business Risk Assessment.....	4
5.2. Customer Risk Assessment.....	4
5.3. Customer Acceptance Policy.....	5
5.4. Customer Due Diligence.....	5
5.5. Ongoing Monitoring.....	6
5.6. Reliance on Third Parties to Perform Customer Due Diligence.....	6
5.7. Reporting of Unusual Transactions.....	6
5.8. Anti-Money Laundering Compliance Program.....	7
6. Compliance and Consequences of Non-Compliance.....	7
7. Related Information.....	7
8. Contact Information.....	8
9. Policy History.....	8
APPENDIX 1.....	9
EPICSTAR B.V. Prohibited Jurisdictions.....	9

1. Policy Statement

Epicstar B.V. ("the Company"), incorporated in Curacao, designed this policy to support the prevention of money laundering (AML), terrorism financing (TF), and the financing of proliferation. The Company implements measures in line with applicable legislation and regulatory expectations of the Curacao Gaming Authority (CGA) and relevant international standards, including those issued by the Financial Action Task Force (FATF).

2. Purpose

- 2.1. This policy is established to prevent the legalization (laundering) of proceeds derived from criminal activities, ensuring these illicit funds do not gain legitimacy through the Company's services. The Company rigorously complies with the anti-money laundering (AML) and counter-terrorism financing (CTF) standards set forth in Curacao's applicable legislation, specifically adhering to:
 - 2.1.1. Identification of Clients in accordance with Curacao Gaming Authority (CGA) AML/CTF guidelines.
 - 2.1.2. Implementation and maintenance of real-time transaction monitoring systems to detect and prevent the placement, layering, and integration of illicit funds.
 - 2.1.3. Prompt and accurate submission of Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) to the Financial Intelligence Unit (FIU) Curacao.
- 2.2. The services provided by Epicstar B.V. are exclusively accessible to individuals acting strictly in their personal capacity. The Company explicitly prohibits transactions or activities conducted by legal entities or representatives acting on behalf of third parties.

3. Audience

- 3.1. This policy applies to all individuals associated with Epicstar B.V., including:
 - All employees of Epicstar B.V.;
 - Subcontractors engaged by Epicstar B.V.;
 - Third-party suppliers providing services to or on behalf of Epicstar B.V.;
 - Individual clients who use or intend to use the services provided by Epicstar B.V..
- 3.2. All parties must comply with the requirements established herein and ensure their activities align with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations applicable under Curacao legislation.

4. Definitions

- 4.1. **AML (Anti-Money Laundering):** Measures and policies aimed at preventing the laundering of money obtained illegally and financing terrorism.
- 4.2. **FT (Financing Terrorism):** Financial support for acts of terrorism or terrorist organizations.
- 4.3. **Client:** An individual (natural person) using the Company's services
- 4.4. **Beneficial Owner:** By using the website, the Client confirms that they are the beneficial owner of the funds used for gaming purposes. A beneficial owner is defined as the individual (natural person) who ultimately owns or controls the funds or assets used in transactions or activities on the platform, acting solely on their own behalf without the involvement of any third party or intermediary.
- 4.5. **KYC (Know Your Client):** A policy for verifying and identifying Clients to assess their risk levels.

- 4.6. **DD (Due Diligence):** A process of investigation or auditing to ensure compliance with laws, regulations, and ethical standards.
- 4.7. **MLRO (Money Laundering Reporting Officer):** A designated individual responsible for overseeing and ensuring the implementation of AML policies and reporting suspicious activities.
- 4.8. **FATF (Financial Action Task Force):** An international organization that sets standards and promotes effective implementation of AML and FT measures.
- 4.9. **OFAC (Office of Foreign Assets Control):** A U.S. government agency that administers sanctions against designated individuals, groups, and entities.
- 4.10. **PEP (Politically Exposed Person):** An individual who holds or has held a high-ranking public office, along with their close associates and family members.
- 4.11. **STR/SAR (Suspicious Transaction Report/Suspicious Activity Report):** Reports filed to regulatory authorities when suspicious or unusual activities are detected.
- 4.12. **FIU (Financial Intelligence Unit):** A government agency responsible for collecting and analyzing information to combat financial crimes like money laundering and terrorism financing.
- 4.13. **Risk-Based Approach:** A method of assessing and managing risks based on their likelihood and impact, especially in Client relationships.
- 4.14. **Sanctioned List:** A list of individuals, entities, or countries subject to trade restrictions or financial penalties.
- 4.15. **Prohibited Jurisdictions:** Countries or regions where the Company is not permitted to conduct transactions due to legal or regulatory restrictions.

5. Policy Implementation

The implementation of this policy is structured to ensure comprehensive compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) obligations. The AML Compliance department holds primary oversight responsibility, manages dissemination, updates, and periodic reviews of this policy.

5.1. Business Risk Assessment

- 5.1.1. The Company systematically assesses all potential and existing money laundering (ML) and terrorism financing (TF) risks. The risk assessment encompasses the following:
 - Evaluating ML/TF risks related to the products and services offered by the Company.
 - Analyzing geographical risks, taking into account the jurisdictions involved in transactions.
 - Identifying potential vulnerabilities associated with customer types and transaction behaviors.
 - Reviewing client information against international sanction lists, including United Nations and other relevant authorities.
- 5.1.2. The Company employs comprehensive data collection tools, including issuing risk assessment questionnaires, to facilitate accurate analysis. Results of the risk assessment guide the adoption and updating of internal policies, controls, and risk mitigation measures. Continuous monitoring ensures the effectiveness and adequacy of these measures.

5.2. Customer Risk Assessment

- 5.2.1. The Company conducts individual customer risk assessments to identify and evaluate specific risks associated with providing its services and products to the Client. This assessment is conducted at the commencement of the business relationship and includes:

- Collection and verification of comprehensive identification data from the Client, such as full name, date of birth, nationality, residential address, and government-issued identification documents (passport, ID card, residence permit).
- Assessment of the legitimacy of the Client's source of funds, supported by appropriate documentation (e.g., bank statements, salary slips, employment or business records).
- Screening of the Client against international sanctions and Politically Exposed Persons (PEP) lists, including but not limited to lists provided by the United Nations, OFAC, the EU, and local Curacao authorities.
- Evaluation of the Client's transactional behavior and expected activities.

5.2.2. The information forms the basis for creating a detailed risk profile, enabling the Company to apply appropriate due diligence measures tailored to the specific risk level identified.

5.3. Customer Acceptance Policy

5.3.1. Based on the outcomes of the Customer Risk Assessment (CRA), the Company applies an appropriate level of Customer Due Diligence (CDD) as defined within its Customer Acceptance Policy (CAP). When formulating and implementing the CAP, the Company strictly complies with its obligations related to Politically Exposed Persons (PEPs) and sanctions screening. Key procedures include:

- Verification of the Client's identity through valid government-issued identification documents and additional supporting documentation.
- Increased control and senior management approval for establishing business relationships with identified PEPs.
- Regular screening against comprehensive international sanctions lists, including those maintained by the United Nations, OFAC, the European Union, and Curacao authorities.
- Clear and documented criteria for declining potential Clients who fail to meet the required CDD standards, including incomplete identity verification, adverse screening outcomes, or suspicion of involvement in prohibited activities.

5.4. Customer Due Diligence

The Company implements appropriate Customer Due Diligence (CDD) measures to comply with relevant regulatory standards and manage risks associated with money laundering and terrorism financing.

- 5.4.1. The Client's identity is verified using valid government-issued identification documents (e.g., passport, ID card, or residence permit).
- 5.4.2. Documentation to support the legitimacy of the Client's source of funds may be requested as necessary, such as bank statements, salary slips, employment or business records.
- 5.4.3. CDD may be applied when a single transaction, or multiple related transactions, amount to NAF 4,000 or more.
- 5.4.4. The Client may be screened against international sanctions lists, including those maintained by the United Nations, Office of Foreign Assets Control (OFAC), the European Union (EU), and Curacao authorities.
- 5.4.5. Enhanced Due Diligence (EDD) may be applied from NAF 5,000 or in cases involving high-risk Clients, such as PEPs or clients from high-risk jurisdictions.
- 5.4.6. EDD procedures may include additional verification steps and potential senior management approval.
- 5.4.7. Reporting and Freezing of Funds: If suspicious activities or sanction-related issues arise, the Company may freeze the Client's funds or restrict account activities. Relevant incidents will be reported promptly to the Financial Intelligence Unit (FIU) of Curacao, following regulatory obligations.

5.5. Ongoing Monitoring

- 5.5.1. The Company maintains procedures to observe the Client's activity and update risk assessments where necessary. Monitoring activities are proportionate to the Client's risk profile.
- 5.5.2. The Company may periodically review identification data and supporting documents submitted by the Client.
- 5.5.3. Updates or re-verification may be requested based on internal risk triggers.
- 5.5.4. Client transactions may be reviewed to ensure consistency with the Client's expected behavior.
- 5.5.5. Unusual or inconsistent activity may lead to additional requests for clarification or documentation.
- 5.5.6. Ongoing Monitoring Triggers:
 - Changes in transaction volume or patterns.
 - External intelligence such as sanctions updates or public exposure.
 - Internal alerts from automated tools or manual review.

5.6. Reliance on Third Parties to Perform Customer Due Diligence

- 5.6.1. The Company may, where appropriate, rely on third-party service providers to perform elements of Customer Due Diligence (CDD), including identity verification and document collection.
- 5.6.2. Third-party providers are selected based on their competence and capacity to follow applicable AML standards.
- 5.6.3. The Company ensures that such providers apply standards broadly consistent with its internal AML policy.
- 5.6.4. The Company retains full responsibility for compliance with AML obligations, even where third-party services are used.
- 5.6.5. The Company may review or audit the procedures applied by third parties.

5.7. Reporting of Unusual Transactions

- 5.7.1. The Company maintains procedures to identify and report transactions that may be considered unusual or suspicious in accordance with applicable laws and the guidelines of the Financial Intelligence Unit (FIU) of Curacao.
- 5.7.2. Transactions should be reviewed using internal automatized tools or manual checks to detect patterns inconsistent with the Client's risk profile or declared activity.
- 5.7.3. The Company should file reports to FIU Curacao for transactions equal to or exceeding NAf 5,000, as required under objective indicators.
- 5.7.4. Transactions below threshold of NAf 5,000 may also be reported based on subjective suspicion.
- 5.7.5. Potentially unusual transactions may be escalated to the designated Money Laundering Reporting Officer (MLRO) for review.
- 5.7.6. The MLRO may request additional information before determining whether a report is necessary.
- 5.7.7. Where applicable, the MLRO may file a Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) through the goAML platform of FIU Curacao.
- 5.7.8. Reporting timelines depend on the applicable indicators and regulatory requirements (e.g., within 24 or 48 hours).
- 5.7.9. Documentation related to reported transactions is retained for the period required by law but not less than five (5) years.

5.8. Anti-Money Laundering Compliance Program

- 5.8.1. The Company maintains an AML Compliance Program aimed at managing risks related to money laundering and terrorism financing. The program is risk-based and is updated as needed.
- 5.8.2. The program includes components such as client due diligence, transaction monitoring, training, internal reporting procedures, and cooperation with competent authorities.
- 5.8.3. The program is intended to reflect the requirements of Curacao AML legislation and applicable international guidelines.
- 5.8.4. Internal controls and measures are designed to be proportionate to the nature, scale, and complexity of the Company's business.
- 5.8.5. Where reasonable grounds exist to suspect ML/TF activity, the Company may block access to personal accounts and/or transactions. Such actions may be taken as part of a risk mitigation response and do not require prior notice to the Client.
- 5.8.6. The AML Program is subject to oversight by the MLRO and may be reviewed periodically or in response to changes in applicable law or risk exposure.

6. Compliance and Consequences of Non-Compliance

- 6.1. The Client is expected to comply with applicable anti-money laundering and counter-terrorism financing regulations, as well as with the Company's internal policies.
- 6.2. Employees and third-party service providers are expected to act in accordance with applicable procedures and regulatory obligations where relevant to their role.
- 6.3. Where the Client fails to comply with AML requirements or where the Client's activity presents a legal or reputational risk, the Company may:
 - Suspend or terminate the business relationship;
 - Restrict or block account access;
 - File reports with regulatory or law enforcement authorities as required by applicable law.
- 6.4. Failure by employees or contractors to follow this policy or relevant laws may result in:
 - Internal disciplinary action, which may include suspension or termination;
 - Notification to competent supervisory authorities;
 - Civil or criminal liability under applicable legislation.
- 6.5. The Company retains discretion in how non-compliance cases are handled and may assess each matter based on the specific facts and applicable legal framework.
- 6.6. This policy does not limit the Company's right to take additional actions as may be required by law or internal risk management decisions.

7. Related Information

This section lists references to applicable laws, guidelines, and internal documents that may assist in interpreting or applying this policy.

- 7.1. Legal and regulatory sources:
 - National Ordinance Reporting of Unusual Transactions (NORUT) - Curacao

- Sanctions National Ordinance (SNO) - Curacao
- Guidance and indicators issued by the Financial Intelligence Unit (FIU) Curacao
- Curacao Gaming Authority AML/CTF Guidelines
- FATF Recommendations: <https://www.fatf-gafi.org>

7.2. International sanctions lists:

- OFAC Sanctions List: <https://sanctionssearch.ofac.treas.gov/>
- EU Consolidated Sanctions List: <https://www.sanctionsmap.eu/#/main>
- UN Sanctions List: <https://www.un.org/securitycouncil/sanctions/un-sc-consolidated-list>

8. Contact Information

Questions regarding the implementation or interpretation of this policy may be directed to the email: compliance@epicstar.net

9. Policy History

This document constitutes the initial version of the AML/CTF Policy for Epicstar B.V. No previous versions apply. Any revisions or future versions will be documented below with effective dates:

- 9.1. Version: IN-AML-029-01, Effective Date: June 16, 2025

APPENDIX 1

EPICSTAR B.V. Prohibited Jurisdictions

Countries List: Abkhazia, Guyana, Tristan da Cunha, Afghanistan, Haiti, Saint Kitts and Nevis, American Samoa, Hong Kong, Saint Vincent and the Grenadines, Anguilla, Iran, Saint-Martin, Antigua and Barbuda, Iraq, Saint-Pierre and Miquelon, Aruba, Isle of Man, Sao Tome and Principe, AUSTRALIA, Jersey, Serbia, Azad Kashmir, Kosovo, Seychelles, Barbados, Libya, Sierra Leone, Bermuda, Lugansk People's Republic, Singapore, Bonaire, Macau, Sint Eustatius, British Virgin Islands, Malawi, Sint Maarten, Canada, Marshall Islands, Slovakia, Cape Verde, Martinique, Solomon Islands, Cayman Islands, Mayotte, Somalia, Chad, Montenegro, South Ossetia, Christmas Island, Montserrat, South Sudan, Cocos (Keeling) Islands, Myanmar, State of Palestine, Comoro Islands, Netherlands, Sudan, Cook Islands, New Caledonia, Sweden, Cuba, Niue, Syria, Curacao, Norfolk, Turkish Republic of Northern Cyprus, Donetsk People's Republic, North Korea, Tokelau, East Timor, Northern Mariana Islands, Transnistria, Eritrea, Palau, Trinidad and Tobago, Falkland Islands, Pitcairn, Turks and Caicos Islands, Faroe Islands, Portugal, Tuvalu, Federated States of Micronesia, Republic of Artsakh, Uganda, France, Republic of the Congo, United Kingdom, French Guiana, Réunion, United States of America (USA), Germany, Crimea, Vatican City, Rwanda, Virgin Islands of the United States, Grenada, Saba, Wallis and Futuna, Guadeloupe, Sahrawi Arab Democratic Republic, Yemen, Guam, Saint Barthelemy, Belgium, Guernsey, Saint Helena, Ascension and, Spain, South Africa, Nigeria, Cambodia, China, Saudi Arabia, Switzerland, Lithuania.