

Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) Policy

1. Policy Statement

Great Star N.V. ("the Company") is fully committed to the highest standards of anti-money laundering (AML) and counter-terrorist financing (CTF) compliance. This policy establishes our framework to prevent the Company and its online gambling operations from being used to facilitate money laundering or terrorist financing, in line with the regulations of the Curaçao Gaming Control Board (GCB), the Financial Intelligence Unit (FIU) Curaçao, and international best practices.

2. Purpose

This policy aims to:

- Prevent and detect potential money laundering or terrorist financing activities.
 - Ensure full compliance with legal and regulatory obligations under Curaçao law.
 - Protect the Company, its customers, and its reputation from abuse by criminal elements.
 - Establish a structured framework for risk assessment, customer due diligence, monitoring, and reporting.
-

3. Audience

This policy applies to:

- All Company employees
 - Third-party service providers
 - Affiliates and subcontractors involved in customer-facing or compliance functions
-

4. Definitions

- **Money Laundering (ML):** The process of disguising the origins of illegally obtained money.

- **Terrorist Financing (TF):** The act of providing financial support to terrorists or terrorist organizations.
- **CDD (Customer Due Diligence):** A process of verifying the identity of customers.
- **EDD (Enhanced Due Diligence):** Additional scrutiny of high-risk customers.
- **FIU:** Financial Intelligence Unit Curaçao, responsible for receiving and analyzing suspicious transaction reports.
- **PEP (Politically Exposed Person):** An individual with a prominent public function, requiring enhanced scrutiny.

5. Policy Implementation

Approving Official(s): Chief Compliance Officer (CCO)

Responsible Office: Compliance Department

Effective Date: 12/5/2025

Next Review Date: [11/5/2026]

5.1 Business Risk Assessment

A comprehensive Business Risk Assessment (BRA) is conducted annually to:

- Identify and evaluate ML/TF risks related to products, services, delivery channels, and geographic locations.
- Ensure policies and procedures are tailored to address these risks.
- Assess the potential misuse of online casino offerings for illegal purposes.

5.2 Customer Risk Assessment (CRA)

Each customer is subject to an individual CRA at onboarding to determine their risk profile. Factors include:

- Geographic risk (High – risk jurisdictions subject to FATF, i.e. Iran, Myanmar)
- Customer behavior (means used for deposits/withdrawals, sum of amounts deposited/ amount per transaction, betting activity, contact with customer service, response regarding verification process)
- Source of funds (annual income, inheritance, sale of property)

- Method of payment (e.g., crypto vs. fiat, e – wallets, cash methods)

5.3 Customer Acceptance Policy (CAP)

Based on CRA outcomes, the CAP ensures:

- High-risk customers undergo EDD
- PEPs and sanctioned individuals are rejected or escalated
In order to avoid such cases, daily checks regarding the registrations are being conducted. Once an individual is proven to be a PEP, the account is immediately blocked, all betting / casino activity is canceled and the amount deposited is refunded back on the payment method used for depositing.
- Sanctions screening is mandatory prior to account activation
Great Star N.V. uses external software / sources such as LexaScan (<https://lexascan.com/>) & EU Sanctions List (<http://www.sanctionsmap.eu/#/main>) in order to prevail against any attempt of registration / financial activity by an individual who has been either sanctioned or under monitoring for illegal activities.

5.4 Customer Due Diligence (CDD)

CDD measures include:

- Collection of full name, address, DOB, ID document, proof of address
- PEP and sanctions screening through automated tools
We, as a company, conduct daily checks in all registrations in order to prevent any registration by a person who can be considered as PEP. These checks may include external software / sources such as OFAC ([HTTPS://OFAC.TREASURY.GOV/SANCTIONS-LIST-SEARCH-TOOL](https://OFAC.TREASURY.GOV/SANCTIONS-LIST-SEARCH-TOOL))
- Freezing of funds and notification to FIU Curaçao when suspicious activity is identified

5.5 Ongoing Monitoring

Continuous monitoring includes:

- Behavioral pattern analysis
- Transaction thresholds and alerts
i.e. in order to be proactive in cases where users proceed to numerous deposits below the company's applied threshold (2000EUR/ transaction) to avoid triggering the CDD procedure. The system flags user as suspicious, the account is immediately frozen, KYC documentation is requested and a notification is being sent to the

MLRO. The account remains in status frozen until user provides the requested documents.

- Login/IP consistency checks
- Unusual withdrawal/deposit behaviors
i.e. Account Take Over cases (ATO) where the account credentials have been sold to a third person. Usually, deposit & betting pattern change, among with payment method.
The account is immediately flagged as suspicious, and extra KYC is required including selfie holding ID/passport, and updated certified official documents issued by public institutions / services.

5.6 Reliance on Third Parties

The Company may rely on licensed third-party providers for CDD, under the condition that:

- Providers meet Curaçao standards
- Responsibility for compliance remains with the Company
- Oversight and audit procedures are in place

5.7 Reporting of Unusual Transactions

All suspicious or unusual transactions are reported to FIU Curaçao through:

- Immediate internal escalation
- Detailed documentation
- Timely SAR / STR (Suspicious Activity / Transaction Report) submission

5.8 AML Compliance Program

The AML Program is designed to:

- Be proportionate to risk level
- Align with Curaçao laws and FATF recommendations
- Include account freezing and reporting mechanisms
- Ensure regular training and compliance reviews

6. Compliance and Consequences of Non-Compliance

Non-compliance may result in:

- Disciplinary actions, including termination

- Regulatory penalties or revocation of license
 - Legal prosecution under Curaçao law
 - Reputational damage
-

7. Related Information

- Curaçao National Ordinance on the Reporting of Unusual Transactions (NORUT)
 - FIU Guidelines
 - Curaçao eGaming AML Handbook
 - Internal CDD/EDD procedure manuals
-

8. Contact Information

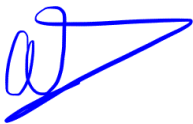
For questions regarding this policy: Compliance Department Email: g.dalianis@gr8star.com Phone: [+30 6942979199]

9. Policy History

- Version 1.0: [12/5/2025] (New Policy)
-

10. Policy URL This policy is published on our corporate website: [Insert URL]

End of Document



eMagnus Curacao B.V.

Managing Director

5/13/2025