

Anti-Money Laundering and Counter-Terrorist Financing Policy

Company Name: Magic Stones N.V.

Registered Address: Dr. H. Fergusonweg 1, 4797, Willemstad, Curaçao

License Number: OGL/2024/566/0462

Regulatory Authority: Curaçao Gaming Authority

Version: 2.0

Effective Date: 01.04.2025

Status: Update Policy

Next Scheduled Review: 31.12.2025

Approved by: UBO Kostiantyn Vatan

Signature _____

MLRO: Mr. Uhnivenko Maksym

Signature _____

Vivian Ersilia o.b.o. (SMES)
Solutions for Management
and Employment Support N.V.

Signature _____

Date: 16.04.2025

Contents

1. Introduction

2. Policy Statement

3. Purpose

- 3.1. Scope and Audience
- 3.2. Legal Framework
- 3.3. Governance and Oversight
- 3.4. Training and Awareness
- 3.5. Review and Maintenance

4. General Terms and Definitions

5. Management and Staff

- 5.1. Management Responsibilities
- 5.2. Role of the MLRO
- 5.3. AML and Anti-Fraud Department
- 5.4. Role of Front-Office Staff
- 5.5. Communication and Escalation

6. Risk Assessment

- 6.1. Business Risk Assessment (BRA)
- 6.2. Customer Risk Assessment (CRA)
- 6.3. Risk Classification and Risk Appetite
- 6.4. Risk-Based Approach and Mitigation Measures

7. Know Your Customer (KYC) and Customer Due Diligence (CDD)

- 7.1. Onboarding and Verification
- 7.2. Beneficial Ownership and Control
- 7.3. CDD Thresholds and Timelines
- 7.4. Refusal or Termination of Relationship
- 7.5. Reliance on Third Parties

8. Enhanced Due Diligence (EDD), Risk Categorization and Sanctions Controls

- 8.1. EDD Triggers and Documentation
- 8.2. Risk Levels and Customer Status
- 8.3. Sanctions Screening and PEP Identification
- 8.4. Delegation and Oversight of CDD Functions

9. Transaction Monitoring and Reporting

- 9.1. Monitoring Tools and Alerts
- 9.2. Escalation and Internal Review Protocol
- 9.3. Suspicious Transaction Reports (STRs)
- 9.4. goAML Reporting and Evidence Retention
- 9.5. Collaboration with Third-Party Monitoring Providers

10. Record Keeping

- 10.1. Retention Categories
- 10.2. Storage Controls and Confidentiality
- 10.3. Integration with Compliance Program

10.4. goAML Record Management

11. Compliance and Consequences of Non-Compliance

12. Related Information and Legal References

13. Contact Information

14. Policy URL

1. Introduction

This Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter – the “Policy”) is adopted by **Magic Stones N.V.**, a company registered at Dr. H. Fergusonweg 1, 4797, Willemstad, Curaçao, license number OGL/2024/566/0462 in accordance with the National Ordinance on Games of Chance. The Policy establishes the internal framework for ensuring full compliance with applicable international standards, EU regulations, national laws of Curaçao, and the requirements of regulatory, supervisory and financial institutions, with the aim of protecting the Company from being used—directly or indirectly—for the purposes of money laundering or terrorist financing.

This Policy applies to all employees, contractors, departments, and business units of the Company, as well as to its financial partners and any relevant third-party service providers involved in the processing of gaming-related transactions.

2. Policy Statement

The Company acknowledges that the online gaming sector may be targeted by criminal actors seeking to conceal the origin of illicit proceeds or to channel funds for terrorist activities. As such, the Company maintains a zero-tolerance approach to money laundering and terrorist financing, and affirms its commitment to the principles of financial integrity, transparency, accountability, and regulatory compliance.

For the purpose of this Policy, **money laundering** is defined as any act designed to conceal the origin of funds derived from illegal activity in order to make them appear legitimate. This includes, but is not limited to:

- the placement of illicit funds into the financial or gaming system;
- layering such funds via structured or obscured transactions;
- the integration of the “cleaned” funds into the economy through withdrawal, investment, or acquisition disguised as legitimate winnings or revenue.

To counter these risks, the Company adheres to the following legal instruments and regulatory frameworks:

- Directive (EU) 2024/1640 and Regulation (EU) 2024/1624;
- FATF 40 Recommendations;
- Curaçao regulatory instruments including NOIS, NORUT, the Sanctions National Ordinance, and the Kingdom Sanctions Act;
- Guidance issued by the Curaçao Gaming Authority and the Financial Intelligence Unit (FIU);
- Payment network standards including Visa VIRP and Mastercard BRAM.

The Company fully complies with these instruments and proactively adapts its internal controls and procedures in line with evolving regulatory obligations.

3. Purpose

This Policy is designed to:

- Establish a uniform approach to AML/CFT obligations across all operations;
- Identify, assess, and mitigate risks associated with money laundering and terrorist financing;
- Outline the responsibilities of staff and management in ensuring compliance;
- Define procedural standards for Customer Due Diligence (CDD), transaction monitoring, reporting of unusual transactions, staff training, and recordkeeping.

The Company implements a robust **risk-based approach (RBA)**, whereby mitigation measures are proportionate to the risks identified. Higher-risk players, transactions, jurisdictions, or delivery channels trigger enhanced due diligence and stricter controls, while low-risk profiles may benefit from simplified procedures, provided this is consistent with legal and regulatory obligations.

3.1. Scope and Audience

This Policy is binding upon all departments, management, operational teams, customer-facing staff, and compliance personnel. It extends to third-party service providers, payment processors, and platform partners whose activities are directly linked to the Company's gaming operations.

Employees are required to understand and comply with all provisions of this Policy. Failure to do so may result in disciplinary actions, including termination, suspension, or escalation to regulatory or law enforcement authorities.

The Company collaborates only with partners and payment providers that demonstrate sufficient AML/CTF controls and are subject to supervision in reputable jurisdictions. Internal communication channels and escalation procedures are implemented to ensure timely and secure reporting of suspicious transactions to the Compliance Department and the FIU.

3.2. Legal Framework

The Policy is developed in accordance with:

- The National Ordinance on Identification of Clients when Rendering Services (NOIS);
- The National Ordinance on the Reporting of Unusual Transactions (NORUT);
- The Sanctions National Ordinance;
- The Kingdom Sanctions Act;
- EU Directive 2024/1640 and Regulation 2024/1624;
- FATF Recommendations and international best practices.

The Company also follows all relevant guidance and instructions issued by the Curaçao Gaming Authority and the FIU.

3.3. Governance and Oversight

Ultimate responsibility for the implementation and enforcement of this Policy lies with the Company's executive management. Day-to-day oversight is delegated to the designated **Compliance Officer**, who operates independently of the gaming operations and reports directly to senior management.

The Compliance Officer is responsible for:

- Maintaining and updating the Policy;
- Ensuring staff training and awareness;
- Monitoring compliance performance;
- Reviewing transactions and investigating unusual activity;
- Filing reports to the FIU and responding to regulatory inquiries.

3.4 Training and Awareness.

The Company ensures that all employees whose roles are relevant to AML/CTF controls receive:

- Mandatory induction training upon joining;
- Periodic refresher training tailored to their duties;
- Role-based training for specialized staff (e.g., cashiers, risk analysts, customer service);
- Updates on legal changes, risk typologies, and red flags.

Training is documented and evaluated for effectiveness. Non-compliance with training obligations is addressed through internal disciplinary procedures.

3.5. Review and Maintenance.

This Policy is reviewed **annually**, or more frequently where:

- There are significant changes in applicable laws or regulations;
- New operational risks or jurisdictions are introduced;
- Deficiencies or breaches are identified through audits or regulatory inspections.

All amendments are reviewed by the Compliance Officer and submitted to senior management for formal approval. The most recent version of the Policy is distributed to relevant staff and made available for inspection by the CGA or FIU upon request.

4. General Terms:

- AML (Anti-Money Laundering): Measures and procedures implemented to prevent, detect, and report money laundering activities.
- CFT (Combating the Financing of Terrorism): Strategies and actions aimed at preventing the provision of financial support to terrorist organizations or activities.
- RBA (Risk-Based Approach): A method of managing compliance obligations by assessing and mitigating risks based on their severity.
- KYC (Know Your Customer/Client): The process of identifying and verifying the identity of a customer to ensure their legitimacy and assess potential risks.
- EDD (Enhanced Due Diligence): Additional measures applied to high-risk customers to address specific risks identified during the KYC process.
- SDD (Simplified Due Diligence): Reduced verification measures for low-risk customers or transactions.
- PEP (Politically Exposed Person): An individual holding a prominent public function or position that may pose higher AML/CFT risks.
- Transaction: Any single deposit or withdrawal made by a customer.
- Deposit: The process by which a customer funds their account to purchase the Company's services.
- Withdrawal: The process of transferring winnings or funds from the customer's account.
- STR (Suspicious Transaction Report): A report submitted to the relevant authorities when suspicious financial activity is detected.
- SAR (Suspicious Activity Report): Similar to STR, focused on broader suspicious activities beyond transactions.
- TPR (Terrorist Property Report): A report filed when property or funds linked to terrorist activities are identified.
- LVCTR (Large Virtual Currency Transaction Report): A report on transactions involving large sums of virtual currency.

Regulatory and Supervisory Bodies

- CBCS (Central Bank of Curaçao and Sint Maarten): The regulatory authority overseeing financial entities and activities in Curaçao and Sint Maarten.
- FIU (Financial Intelligence Unit of Curaçao): The national agency responsible for receiving and analyzing suspicious transaction reports (STRs).

- FATF (Financial Action Task Force): An international body that sets global standards for combating money laundering and terrorist financing.

Roles and Responsibilities

- MLRO (Money Laundering Reporting Officer): The individual responsible for overseeing AML compliance and reporting within the Company.

- CO (Compliance Officer): A designated employee tasked with ensuring that the Company adheres to AML/CFT policies and procedures.

- CSAF (Customer Support and Anti-Fraud): A department within the Company responsible for addressing customer queries and monitoring for fraudulent activity.

Legislation and Regulations:

- NORUT (National Ordinance Reporting Unusual Transactions): Curaçao's legal framework for the reporting of unusual financial transactions.

- PCMLTA (Proceeds of Crime (Money Laundering) and Terrorist Financing Act): A legal framework governing AML/CFT measures.

- PCMLTFR (Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations): Regulatory provisions supporting PCMLTA.

Other Key Terms:

- FI (Financial Institution): Any entity that facilitates financial transactions, including banks and payment gateways.

- Principal (Antillephone, N.V.): The designated service provider licensed to facilitate gaming operations.

- Anonymous Payment Methods: Payment methods such as prepaid cards or cryptocurrencies that provide limited traceability.

- UBO (Ultimate Beneficial Owner): The individual(s) who ultimately own or control a company or account.

- Withdrawal Limits: Restrictions set to monitor and control the flow of funds from a customer's account

5. MANAGEMENT AND STAFF

5.1. MANAGEMENT

The Company's AML and CFT compliance structure is built on the joint oversight of a Senior Manager and a Compliance Officer. Depending on the scale and complexity of operations, these functions may be fulfilled by the same individual, subject to the owner's decision. Senior management bears ultimate responsibility for ensuring the adequacy of governance arrangements necessary to mitigate ML/TF risks.

The Senior Manager must maintain a clear and current understanding of the Company's exposure to such risks and ensure the adoption of appropriate systems and internal controls. This includes regular oversight of the Company's AML/CFT framework, validation of the Compliance Officer's appointment, and assurance that the CO possesses the requisite expertise and independence. The Senior Manager is responsible for the provision of sufficient resources, the facilitation of access to customer information and transactional data, and the clear communication of reporting channels within the organization. Furthermore, the Senior Manager evaluates the CO's annual compliance report, acts upon identified deficiencies, and responds to findings from internal audit reports with remedial measures as necessary.

The Compliance Officer ensures that the Company's internal compliance systems remain responsive to both regulatory requirements and operational realities. Acting as an advisor to senior management and a strategic partner to the MLRO, the CO oversees the maintenance, development, and review of AML/CFT procedures. The CO monitors the effectiveness of internal controls, advises on compliance strategy, and ensures the adequacy of operational resources. Additional duties include employee awareness, the supervision of training programs, the timely submission of the Annual Compliance Report, alignment with evolving regulations, cooperation with internal audit, and coordination with third-party stakeholders such as financial institutions and payment providers.

The Money Laundering Reporting Officer (MLRO) is directly responsible for the execution of the Company's AML/CFT framework and serves as the primary liaison with external authorities. Mr. Uhnivenko Maksym currently holds this role. The MLRO ensures the effective operationalization of compliance measures, supervises the handling and external reporting of suspicious transactions, and verifies that payment providers fulfill their reporting obligations in a timely and accurate manner. The MLRO monitors the application of due diligence procedures by the payment gateway, including KYC, EDD, and ongoing monitoring. He remains responsible for the coordination of risk assessments, daily monitoring of compliance-related activity, documentation retention, internal training, and external cooperation with law enforcement and supervisory authorities. The Company will duly notify the authorities and update this Policy should a change in MLRO appointment occur.

The Company's AML/CFT program is subject to periodic independent review. An external audit or qualified internal function independent of the AML operations shall assess the adequacy and effectiveness of AML controls and procedures at least once per year. Findings

and recommendations are reported to Senior Management, and corrective measures are implemented where necessary to ensure continuous improvement and regulatory alignment

5.2. Role of the Money Laundering Reporting Officer (MLRO)

The Company appoints a Money Laundering Reporting Officer (MLRO) as the designated individual responsible for the practical implementation and oversight of its anti-money laundering and counter-terrorist financing framework. At present, this function is performed by Mr. Uhnivenko Maksym. Any changes in this appointment will be duly communicated to the competent authorities and reflected in the present Policy.

The MLRO serves as the central figure in ensuring the operational effectiveness of the Company's AML/CFT program and acts as the official liaison with regulatory and law enforcement bodies. His role encompasses the continuous translation of strategic compliance principles into concrete procedures and controls embedded across the Company's activities. This includes verifying that all suspicious activity detected via the payment gateway is promptly analyzed, duly documented, and reported to the appropriate external authorities in accordance with applicable legislation. The MLRO is responsible for ensuring that reporting obligations are fulfilled with accuracy, completeness, and within prescribed timelines, while also maintaining the integrity of all related records and communications.

As part of his mandate, the MLRO supervises the gateway's application of customer due diligence, including enhanced due diligence measures for high-risk individuals and jurisdictions. He reviews the adequacy of implemented KYC, transaction monitoring, and ongoing verification mechanisms, and ensures timely remediation of any deficiencies revealed through ongoing oversight. Furthermore, he is charged with conducting risk assessments tailored to the Company's operational structure, with the objective of identifying systemic vulnerabilities and introducing proportionate mitigating actions.

In the course of daily operations, the MLRO monitors the consistency of internal compliance activities, reviews alerts and escalations, and guarantees that any deviation from established procedures is swiftly addressed. He maintains structured cooperation with external financial institutions, payment providers, and technical partners, ensuring harmonized implementation of control mechanisms across all transactional channels.

Additionally, the MLRO assumes responsibility for the secure and orderly retention of compliance-related documentation, including training logs, transaction records, and all communications with authorities. He ensures that these records remain available for inspection at the request of the CGA or any other competent supervisory body. Finally, the MLRO oversees the pre-employment screening of relevant personnel and coordinates mandatory training programs to maintain a high level of AML/CFT awareness and procedural competence across the organization.

5.3. AML and Anti-Fraud Department

The AML and Anti-Fraud Department operates under the direct coordination of the Money Laundering Reporting Officer, forming an integral component of the Company's compliance infrastructure. Its functional mandate encompasses the detection, prevention, and mitigation of fraud and cybercrime risks, ensuring full integration with AML/CFT controls and internal reporting obligations. Leveraging advanced technical tools such as **Sum&Substance and NameScan**, the Department carries out real-time screening, identity verification, and risk scoring, with a particular emphasis on identifying politically exposed persons (PEPs), sanctioned individuals, and jurisdictional anomalies. Supplementary resources, including official open-source government registries and world leadership directories, are routinely consulted to strengthen the accuracy of risk assessments and verification procedures.

Within its scope, the Department maintains direct oversight of automated KYC processes, ensuring the consistency, completeness, and validity of all identification data collected at onboarding and throughout the customer lifecycle. All irregularities, anomalies, or flags generated by automated systems are subject to manual verification and are escalated where appropriate. The Department investigates and documents all incidents of suspected fraudulent behavior, manages chargeback-related queries, and cooperates with payment partners to ensure financial and reputational risks remain contained. The performance and adequacy of fraud detection strategies are regularly evaluated, with reports submitted to the MLRO for further review and system refinement. Where procedural inefficiencies or operational blind spots are detected, the Department advises on corrective measures and facilitates the implementation of improved controls across the Company's platforms.

5.4. Role of Front-Office Staff

The Company's front-office personnel, primarily represented by Customer Support and Account Management functions, serve as the initial interface between the platform and its clients. Owing to the nature of their responsibilities, these employees may become the first to observe behavioral anomalies or indicators of manipulation by customers attempting to circumvent AML/CFT safeguards. Recognizing this exposure, the MLRO and Compliance Officer deliver structured and recurrent training to front-office staff, equipping them with practical tools to detect red flags, respond appropriately, and channel concerns through formal compliance pathways.

Front-office staff are explicitly prohibited from informing customers of any internal investigation or pending suspicious transaction report ("tipping off"). This prohibition applies even when inquiries or account restrictions may appear unexpected to the customer.

Front-office teams support the execution of customer due diligence by assisting users in the submission of identification documents and clarifying procedural requirements where needed. They are responsible for the accuracy and timeliness of customer account updates and for ensuring that user interactions remain within the bounds of regulatory and operational guidelines. Where customer behavior raises suspicion, or where activities deviate from established profiles, front-office staff are required to escalate such matters to the AML and Anti-Fraud Department for further assessment. In addition, they are trained to

recognize and report potential security breaches or fraudulent access attempts, ensuring that any concern is promptly transmitted to the responsible function for appropriate resolution. Through continuous training, direct engagement, and adherence to internal escalation protocols, front-office teams reinforce the integrity of the Company's first line of defense.

5.5. Communication and Escalation

The Company maintains clearly defined communication and escalation procedures to facilitate the timely and confidential reporting of compliance-related incidents, including unusual transaction patterns, procedural violations, and exposure to high-risk activities. All employees are obligated to report identified concerns without delay using designated internal channels, with direct access to either the Compliance Officer or the Money Laundering Reporting Officer depending on the nature and sensitivity of the issue. The confidentiality of all such reports is guaranteed by internal policy, and retaliatory actions against whistleblowers are strictly prohibited.

Escalation protocols are designed to ensure that all relevant facts are promptly assessed, appropriately classified, and addressed within the shortest operational timeframe possible. Where matters involve significant compliance implications, Senior Management is promptly informed and involved in resolution measures. The effectiveness of these communication and escalation systems is subject to periodic review by executive leadership, ensuring continued alignment with evolving regulatory standards and operational realities. This framework reinforces internal accountability and supports a culture of transparency, diligence, and proactive risk management.

6. Risk Assessment

The Company maintains a comprehensive and adaptive risk assessment framework designed to identify, evaluate, and mitigate risks related to money laundering and terrorist financing that may arise within its operational structure. This framework is developed in accordance with international AML/CFT standards and is calibrated to address the specific vulnerabilities inherent in the online gambling sector. Central to this framework is the application of a Risk-Based Approach (RBA), which enables the Company to allocate resources proportionally to the level of risk identified across customers, transactions, jurisdictions, and products. Emphasis is placed on high-risk areas to ensure that mitigation efforts are both effective and operationally sustainable.

The Company's Business Risk Assessment is developed in alignment with the National Risk Assessment (NRA) of Curaçao and the Sectoral Risk Assessment issued by the relevant authorities. These sources guide the identification and weighting of risk factors specific to the gaming sector and inform the design of risk mitigation measure

In accordance with the RBA, the Company continuously assesses and recalibrates its risk evaluation methodologies to reflect evolving typologies, regulatory changes, and geopolitical developments. This dynamic approach ensures that internal controls remain targeted, proportional, and reflective of the actual exposure profile. Customers are individually risk-rated based on behavioral patterns, transactional activity, and geographical connections, with particular attention given to deviations from expected norms. Enhanced due diligence is applied where elevated risk is identified, and ongoing monitoring procedures are deployed to detect shifts in customer conduct or profile.

The Company acknowledges that geographic exposure is a critical determinant of ML/TF risk. A structured geographic risk model is employed to evaluate countries and regions based on a range of indicators, including the existence of international sanctions, prevalence of criminal activity, proximity to financial crime corridors, and the strength of local AML supervision. The Company does not enter into or maintain business relationships with individuals or entities associated with jurisdictions deemed high-risk, sanctioned, or non-cooperative. This prohibition extends to a number of countries listed in the internal register, which is regularly reviewed and updated in line with international advisories and the Company's internal assessments. All attempted interactions linked to such jurisdictions are systematically blocked, escalated to the MLRO or Compliance Officer, and, where applicable, reported to competent authorities.

Further, the Company considers the nature and complexity of its products and services as potential amplifiers of inherent risk. Products that facilitate anonymity, involve high volumes, or enable rapid cross-border transactions are subject to heightened scrutiny. The use of advanced payment technologies, including e-wallets, digital assets, and mobile interfaces, is continuously monitored through dedicated systems to detect unusual or potentially suspicious patterns. Prior to the introduction of any new product or service, a formal risk evaluation is conducted to determine the potential AML/CFT exposure and the adequacy of proposed mitigation measures.

The Company's risk mitigation structure integrates system-based transaction screening tools, specialized staff training, procedural safeguards, and escalation mechanisms that ensure full traceability, accountability, and regulatory transparency. Training programs are designed to reinforce staff awareness of jurisdictional risks and typologies associated with high-risk products. Compliance actions are documented in a manner that allows for full auditability and supervisory review.

Through the rigorous implementation of this risk assessment framework, the Company upholds its regulatory obligations, reinforces the integrity of its operations, and safeguards the interests of all stakeholders. This proactive approach demonstrates the Company's commitment to maintaining a secure and compliant gaming environment resistant to criminal exploitation.

7. Know Your Customer (KYC) and Customer Due Diligence (CDD)

The Company has established and applies a robust Know Your Customer (KYC) and Customer Due Diligence (CDD) framework, which is fundamental to identifying legitimate customers, assessing risk exposure, and preventing the misuse of its services for money laundering or terrorist financing purposes. These procedures are implemented in accordance with Directive (EU) 2024/1640 and other applicable regulations and are tailored to the risk profile of the Company's operational model within the online gambling industry.

CDD measures are mandatorily applied when individual or aggregated transactions reach or exceed the **amount of EUR 2,000** or consistency with local thresholds, the Company acknowledges the NAF 4,000 regulatory threshold applicable under Curaçao law, and treats it as equivalent to EUR 2,000 for procedural alignment. Upon triggering this threshold, the customer is required to complete the due diligence process, which includes the submission of identifying information and, where applicable, supporting documents. Customers who are subject to CDD may face temporary restrictions on their accounts until the process is completed. In cases where the requested verification is not completed within thirty calendar days, the customer's account is closed, and any remaining funds are returned to the original funding method, unless restricted by a regulatory obligation or a suspicious transaction report (STR). If a staff member identifies signs of potential money laundering or terrorist financing, the matter is escalated to the **MLRO**, who determines whether an internal report warrants the filing of an **STR with the FIU Curaçao**.

Customer onboarding begins with the online registration process, during which each new applicant is required to provide an email address and password. Additional contact details may be requested. Access to the platform is restricted until the customer completes mandatory email verification. At this stage, the system performs automatic checks for duplicate accounts, self-excluded users, and geographic restrictions. **The IP address is logged and reviewed to identify prohibited jurisdictions.** Any account found to be linked to such jurisdictions is blocked immediately. Further, accounts suspected of duplication are suspended pending manual review.

The Company maintains a strict age policy. Individuals **under the age of 18 are prohibited** from registering. The system architecture is configured to detect and prevent underage access. The Company continuously assesses external technological solutions that assist in age and identity verification and integrates such tools where appropriate to enhance the effectiveness of its controls.

Where doubts arise during the registration process or during the course of the relationship, the Company may request additional documentation, including valid government-issued identification, proof of residential address, and, if relevant, verification of payment method. These documents are reviewed by authorized AML personnel in accordance with established procedures. If the information provided remains inconclusive, the MLRO is

consulted to determine appropriate follow-up actions. All collected documents are stored in compliance with applicable data retention and confidentiality rules and are accessible to regulatory authorities upon request.

Each customer is subject to continuous monitoring throughout the relationship. Transactional activity, changes in behavior, and external indicators may trigger a re-evaluation of risk. Where inconsistencies, suspicious activity, or indicators of elevated risk are observed, enhanced due diligence (**EDD**) measures are applied without delay. EDD is also mandatory when a customer's cumulative annual deposits exceed **EUR 10,000**, regardless of other risk factors.

In addition to verifying the identity of the customer, the Company undertakes reasonable measures to determine whether the customer is acting on behalf of another natural person or legal entity. Where a beneficial owner is identified, the Company collects and verifies such individual's identity in accordance with applicable due diligence standards. Verification of ultimate beneficial ownership is conducted through documentary evidence or reliable independent sources and recorded in the customer's due diligence file.

The Company strictly prohibits the establishment or continuation of business relationships with individuals or entities who refuse to comply with verification procedures, attempt to maintain anonymous or third-party accounts, or are known or suspected to be politically exposed persons or individuals subject to international sanctions. Any such attempts are documented, escalated, and reported as required under law.

The Company's KYC and CDD procedures are reinforced by automated systems, internal oversight, and compliance review mechanisms. A complete record of the customer's verification history is maintained for the duration of the relationship, along with all updates and case notes. These records form the basis for auditability, accountability, and transparency, and ensure that the Company is able to demonstrate full compliance with applicable AML/CFT obligations.

8. Enhanced Due Diligence (EDD), Customer Risk Classification and Sanctions Controls

In accordance with its obligations under Directive (EU) 2024/1640 and the applicable national framework, the Company applies Enhanced Due Diligence (EDD) in situations where a customer presents a heightened risk of money laundering or terrorist financing. EDD is triggered where there are inconsistencies or anomalies in the customer's application, when the cumulative **amount of deposits exceeds EUR 10,000**, or where the customer is suspected of belonging to a high-risk or prohibited category, including politically exposed persons (PEPs) or individuals associated with sanctioned jurisdictions. All EDD procedures are carried out under the direct supervision of the MLRO.

Where EDD is applied, the customer is required to submit a certified copy of a government-issued identification document, which may be in the form of an international passport, a local ID accompanied by a notarized English translation, or a live photo of the customer holding such a document. Proof of residential address, not older than three months, must also be provided in the form of a utility bill issued in English or accompanied by a certified translation. In cases where the customer's total annual deposits **exceed EUR 100,000**, a documented and verifiable source of funds is required. All documents are subject to verification through automated systems including Sum&Substance and NameScan, and are reviewed by the AML and Anti-Fraud Department. Where concerns remain, the MLRO issues a written determination, which is retained in the customer file for a minimum of five years following the termination of the business relationship.

If the customer fails to provide the requested documentation, or submits falsified materials, the Company shall terminate the relationship and refund any remaining funds exclusively to the payment instrument originally used for deposit. In cases where such refund is not feasible for legitimate technical or legal reasons, the MLRO may authorize an alternative payout method by written resolution, which must be documented and retained for a period of no less than five years.

Each customer is classified according to an internal risk-based status framework. New Players are those who have registered but not completed profile verification and whose total annual deposits remain below EUR 2,000. Verified Players are customers who have passed initial verification and may deposit up to EUR 10,000 annually. Enhanced Verified Players are those whose cumulative deposits meet or exceed EUR 10,000 and who have successfully completed the EDD process. Active Players are Enhanced Verified Players who have made at least ten transactions in a year, including at least one withdrawal, and whose total deposits fall between EUR 10,000 and EUR 100,000. VIP Players are those whose total deposits exceed EUR 100,000 annually. Where the cumulative deposit volume exceeds EUR 1,000,000 within a six-month period, the Company may recommend voluntary temporary suspension of activity, accompanied by a refund of outstanding balances. Rejected Players are those who fail or refuse to comply with the Company's due diligence requirements or who are deemed ineligible under the Company's risk criteria.

The Company does not engage with individuals or entities located in sanctioned or high-risk jurisdictions, those attempting to act on behalf of undisclosed third parties, or those who request the use of cash or anonymous instruments. Any attempt to establish a relationship under such circumstances is denied and documented

All customers are screened against global sanctions and PEP lists using automated systems including NameScan, and publicly available databases such as the UN Security Council Consolidated List, the EU Consolidated List, the US OFAC sanctions lists, and the FinCEN advisory list. A PEP is defined as an individual entrusted with a prominent public function,

including but not limited to heads of state or government, senior judicial or military officials, members of parliament or high-level regulatory bodies, executives of state-owned enterprises, and directors of international organizations. Where a customer is identified as a PEP or a close associate or family member of a PEP, EDD measures are immediately applied, and the customer is treated as high-risk. In cases where such profiles coincide with sanction exposure, the Company will reject the business relationship and report the attempt in accordance with regulatory obligations.

For the purposes of verifying political exposure and identifying persons of public interest, the Company additionally utilizes the following official and open-access resources:

<https://namescan.io/FreePEPCheck.aspx>.

<https://www.cia.gov/resources/world-leaders>.

<https://www.rulers.org>.

<https://www.knowyourcountry.com>.

and regional references such as the PEP Caribbean List where applicable.

The Company may, where appropriate, delegate specific components of the KYC and CDD process to third-party service providers, provided that such delegation does not diminish the Company's responsibility for regulatory compliance. All third-party providers are subject to due diligence, contractual safeguards, and ongoing audits to ensure adherence to the Company's policies and applicable legal obligations. When outsourcing verification processes, the Company ensures that all personal data is handled in accordance with its Privacy Notice and relevant data protection legislation.

The Company's EDD framework is integrated with its general risk management architecture and serves as a critical control in preventing the exploitation of its services by illicit actors. EDD outcomes, including risk determinations and written resolutions, are centrally recorded, subject to review by the MLRO, and made available to supervisory authorities as required. Through the implementation of these measures, the Company maintains a secure and compliant environment in which operational integrity and customer protection are fully preserved.

9. Transaction Monitoring

The Company maintains a structured and risk-sensitive transaction monitoring framework to detect, prevent, and report suspicious activities potentially associated with money laundering or terrorist financing. While technical responsibility for transaction-level oversight is partially delegated to certified third-party payment service providers, the Company retains responsibility for user-level behavior monitoring and ensures effective two-way coordination with its external partners. The Company guarantees that all monitoring activities, whether internal or external, are aligned with applicable international

and local AML/CFT standards, including FATF Recommendations and the requirements of the Curaçao Financial Intelligence Unit (FIU Curaçao).

The Company utilizes advanced technical tools and monitoring platforms, integrated with its KYC and CDD infrastructure, to flag anomalies that may indicate ML/TF risks. Suspicious behavior may include high-frequency transactions, unusual structuring, use of multiple accounts or payment instruments, and interactions with high-risk jurisdictions. Alerts are generated based on pre-established criteria and are subject to review by the AML and Anti-Fraud Department.

Where unusual activity is detected, the matter is escalated through a multi-step protocol designed to ensure timely analysis, appropriate coordination with payment providers, and accurate reporting where necessary. All employees are trained to recognize signs of suspicious behavior and are obligated to report any concerns to the AML and Anti-Fraud Department without delay.

9.1. Escalation and Internal Review Protocol

1. **Detection of Unusual Activity:** irregular or inconsistent transaction behavior is identified either internally or by a third-party gateway system.
2. **Preliminary Review:** the AML and Anti-Fraud Department assesses the alert to determine whether it reflects legitimate activity or requires further investigation. Factors such as PEP status, geographic exposure, or behavioral deviation are considered.
3. **Compliance Officer Review:** where initial review indicates material concern, the case is escalated to the Compliance Officer, who conducts a risk-based assessment and initiates coordination with external providers where appropriate.
4. **Engagement with Payment Providers:** the Company communicates relevant customer and transaction data to the third-party provider to obtain detailed transaction-level insights. These interactions are securely documented and retained.
5. **Final Review and STR Decision:** where suspicion remains unresolved, the matter is escalated to the Money Laundering Reporting Officer (MLRO), who evaluates all available information and determines whether a Suspicious Transaction Report (STR) should be filed with FIU Curaçao.
6. **Follow-Up and Mitigation:** if an STR is filed, the affected account may be temporarily restricted or subject to enhanced monitoring. Internal systems and procedures are updated to reflect any identified control weaknesses or emerging threats.

All escalation steps, including staff involvement and communications with external entities, are recorded in accordance with legal retention requirements. All documents related to the escalation, review, and filing process are retained for a minimum of five years. Confidentiality is ensured throughout the process, and whistleblower protections apply to all staff reporting in good faith.

9.2. Suspicious Transaction Reports (STRs)

An STR is submitted to FIU Curaçao when the MLRO determines that there are reasonable grounds to suspect that a transaction is associated with money laundering or terrorist financing. This decision is based on a structured evaluation of three components:

- **Facts:** Concrete, verifiable data including dates, amounts, payment methods, and identities of involved parties;
- **Context:** Circumstances or patterns that may indicate deviation from expected behavior;
- **Indicators:** Red flags such as structured deposits, geographic anomalies, unverified sources of funds, or links to sanctioned individuals or jurisdictions.

The STR must present the case clearly enough for another trained AML professional to reach the same conclusion under similar conditions. STRs are filed promptly once the threshold of “reasonable grounds to suspect” (RGS) is met.

9.3. Contents of an STR

Each STR must include, where applicable:

- Customer identification details and relationship to the Company;
- Transaction amounts, types, methods, and timing;
- Explanation of the suspicious elements and reasoning;
- Associated documents and evidence (e.g., KYC files, transaction logs);
- A record of any attempted transactions that were not completed;
- Summary of actions taken prior to reporting.

All STRs are submitted electronically to FIU Curaçao using the designated platform (e.g., goAML) and are monitored for acknowledgment and follow-up where required.

9.4. Collaboration with Third-Party Monitoring Providers

The Company maintains active partnerships with third-party payment and risk analysis providers that are responsible for real-time transactional screening. These providers must demonstrate compliance with international AML/CFT standards and are subject to periodic audits initiated by the Company. Specific provisions include:

- Adherence to FATF-aligned screening methodologies;
- Secure, encrypted data exchange protocols;
- Immediate escalation of high-risk transactions to the Company’s Compliance Officer;
- Availability of full transactional audit trails for review by the Company or authorities;
- Capability to screen and escalate transactions linked to PEPs, sanctioned individuals, or high-risk jurisdictions.

All collaboration is governed by service-level agreements that define roles, responsibilities, escalation mechanisms, and confidentiality obligations. The Company ensures that each provider maintains adequate resources, infrastructure, and regulatory alignment to fulfill its monitoring mandate.

10. Record Keeping

The Company maintains a comprehensive record-keeping framework that ensures full traceability of customer activity, internal decision-making, and regulatory compliance processes. All records are retained in accordance with applicable laws, including Curaçao's AML Ordinances, EU Directive 2024/1640, and FIU guidelines. The primary objective of this framework is to facilitate the reconstruction of customer transactions, due diligence reviews, internal decisions, and interactions with authorities, particularly in the context of audits, investigations, or legal proceedings.

The Company is required to retain all customer and transactional records for a minimum of **five (5) years** following the termination of the business relationship or the completion of an occasional transaction. For certain high-risk files, including those involving Enhanced Due Diligence (EDD) or Suspicious Transaction Reports (STRs), the retention period shall not be less than **seven (7) years**.

10.1. Categories of Retained Records

The following categories of documentation are retained securely and in a readily retrievable format:

- **Customer Identification and Verification Data:**
Copies or digital equivalents of all identity documents collected during onboarding, including passports, ID cards, proof of address, and, where applicable, certified translations or selfies with ID. Where physical copies are not retained, references to the data source and verification method are required.
- **Due Diligence and Monitoring Records:**
Documentation related to the application of CDD and EDD procedures, including notes of investigative actions, summaries of risk evaluations, customer risk classification, and any temporary or permanent account restrictions applied.
- **Transaction Records:**
Full logs of financial activity conducted through or via the Company, including deposits, withdrawals, payment instrument details, IP geolocation logs, and timestamps, whether or not the transaction triggered a verification threshold.
- **Compliance Documentation:**
Internal resolutions issued by Senior Management, the MLRO, or the Compliance Officer concerning high-risk clients, reporting obligations, escalation decisions, or the delegation of responsibilities.
- **STR/SAR Files:**
Reports prepared by the MLRO, whether submitted or not, including the rationale

behind the final determination, underlying evidence, and any correspondence with FIU Curaçao or other competent authorities.

- **Training and Policy Documents:**

Records confirming AML/CFT training sessions conducted for staff, including attendance logs, materials used, and periodic refreshers. Updated versions of this Policy and its supporting procedures are also retained.

- **Law Enforcement and Regulatory Correspondence:**

All formal communications from or to law enforcement bodies, the CBCS, Principal, FIU Curaçao, and other supervisory entities. This includes letters, notices, inquiries, responses, and internal memoranda documenting how such correspondence was addressed.

- **Internal Reports Not Acted Upon:**

Where an internal alert or suspicious activity was reviewed but not escalated to the FIU, a written explanation must be retained outlining the justification for no further action.

10.2 Retention Standards and Controls

All records are stored securely, with access limited to authorized personnel. Records must be clearly indexed and recoverable without undue delay in response to supervisory inspection or legal demand. In cases where records are digitized, appropriate backup and cybersecurity measures are enforced to ensure data integrity and confidentiality.

Where the Company engages third-party providers or cloud-based solutions to store or process records, it ensures that such arrangements include contractual obligations relating to data protection, availability, access controls, and regulatory compliance.

Employees are prohibited from destroying, altering, or concealing any compliance-related record during the retention period. Exceptions must be approved by the MLRO in writing and must not contravene applicable laws or reporting obligations.

For further procedural guidance, employees are instructed to consult the Company's **Due Diligence and Data Management Procedures**, which provide detailed operational standards regarding the classification, storage, and auditing of compliance records.

10.3. goAML Reporting

In accordance with the requirements of the Financial Intelligence Unit of Curaçao (FIU Curaçao), the Company utilizes the **goAML electronic reporting system** for the submission of Suspicious Transaction Reports (STRs) and other required disclosures. This system ensures secure, standardized, and traceable communication between the Company and the FIU, as mandated by local AML legislation and administrative guidance.

All STRs, whether initiated internally or as a result of escalations from third-party providers, are uploaded to the goAML platform by the MLRO or a delegated individual acting under the MLRO's authority. The Company ensures that access to goAML is restricted

to trained and authorized personnel only, and that all such individuals are registered and approved users within the system.

Each report submitted via goAML includes structured data and supporting documentation, such as customer identification records, transactional details, behavioral analysis, and internal escalation notes. Reports must be submitted promptly upon the formation of reasonable grounds to suspect money laundering or terrorist financing. The MLRO ensures compliance with all technical and timing requirements associated with goAML reporting.

Confirmation of receipt by the FIU, follow-up queries, and responses from the authorities are logged and retained alongside the corresponding STR file. Where feedback is provided by the FIU regarding the quality or completeness of a report, the Company records the issue and incorporates corrective measures into future reporting processes.

The Company maintains a full audit trail of all submissions through goAML, including submission timestamps, user activity logs, and any system correspondence. These records are retained for a minimum of **seven (7) years** and are available for inspection by regulatory or law enforcement authorities upon request.

11. Compliance and Consequences of Non-Compliance

Compliance with this Policy is mandatory for all employees, managers, contractors, and any third parties acting on behalf of the Company. Non-compliance with AML/CFT obligations may expose the Company to significant regulatory, financial, and reputational risks, and may constitute a criminal offence under applicable legislation.

Failure to adhere to the procedures outlined in this Policy, including those related to customer due diligence, transaction monitoring, record-keeping, or the reporting of suspicious transactions, may result in internal disciplinary measures, up to and including termination of employment or business relationship. Where applicable, violations may also be reported to the relevant regulatory or law enforcement authorities.

The Company maintains a zero-tolerance approach toward willful misconduct, gross negligence, or any attempt to circumvent AML/CFT controls. Internal audits and monitoring activities are conducted to ensure policy adherence. Staff members are encouraged to report violations in good faith, and such reports are protected under whistleblower provisions.

12. Related Information

This Policy should be read in conjunction with the following documents and instruments, which provide further guidance and operational requirements:

- Curaçao National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Curaçao National Ordinance on the Identification of Clients when Rendering Services (NOIS)
- Sanctions National Ordinance and Kingdom Sanctions Act
- Directive (EU) 2024/1640 and Regulation (EU) 2024/1624
- FATF 40 Recommendations
- goAML Reporting Guidelines (FIU Curaçao)
- AML Risk Assessment Matrix and Internal Escalation Flow
- Internal Due Diligence Procedures and Client Acceptance Guidelines
- AML Training Records and Staff Declaration Logs

These instruments provide detailed operational standards and form part of the Company's AML Compliance Program

13. Contact Information

For any questions or clarification regarding this Policy or the Company's AML/CFT obligations, please contact:

Compliance Department

Magic Stones N.V.

Dr. H. Fergusonweg 1, 4797, Willemstad, Curaçao

Email: ks.vatan@magic365.com

MLRO: Mr. Uhnivenko Maksym

Email: j.compliance@magic365.com

14. Policy URL

The current version of this Policy is available online via the internal compliance portal or may be requested in digital format via j.compliance@magic365.com.

If published, the Company's external-facing policy documentation may be accessed at: www.magic365.com

Annex 1 – Customer Risk Assessment Matrix

This annex outlines the Company's internal risk classification model used to assess the exposure presented by each customer. The matrix applies to both new and experienced players and informs the application of due diligence measures proportionate to the customer's risk level. It is reviewed and maintained by the Compliance Department under the supervision of the MLRO.

Risk Parameter	Low Risk	Medium Risk	High Risk
Jurisdiction	EU/EEA countries, low-risk jurisdictions	Transitional risk countries	Sanctioned or high-risk jurisdictions
Age	25–55 years old	18–24 or 56–65	<18 or >65 (falsified or unverifiable)
PEP/Sanctions	None detected	History of proximity to PEP	Customer is a PEP or appears on a sanctions list
Transaction Volume	<2,000 EUR	2,000–10,000 EUR	>10,000 EUR annually
Deposit-Withdrawal Pattern	Stable or gaming-consistent flow	Occasional full withdrawal	Frequent full withdrawals shortly after deposit
Changes in Profile	No change since registration	Email or payment method updated once	Frequent or unexplained changes
Gaming Behaviour	Consistent session patterns	Short bursts of high betting	Irregular logins, large bets, early exits
Reversal/Chargebacks	None reported	One confirmed reversal	Multiple chargebacks or complaints
Account Origin	One device, one IP	Multiple IPs within same country	Multiple IPs, cross-border logins
Due Diligence Action	Accept account, periodic review	Apply standard CDD, monitor	Apply EDD, escalate to MLRO, possibly block

Annex 2 – Enhanced Due Diligence (EDD)

This matrix outlines the triggers and procedures for Enhanced Due Diligence (EDD) applied to high-risk customers. EDD is mandatory when specific risk indicators are detected, as outlined below.

EDD Trigger	Required Documentation	Actions to Be Taken
Customer exceeds EUR 10,000 annual deposit	Government-issued ID, Proof of Address	Apply EDD, flag for periodic review
Customer identified as PEP	ID, address, Source of Funds	Immediate MLRO escalation, potential rejection
Customer from high-risk jurisdiction	ID, address, SOF with third-party confirmation	EDD, temporary restriction pending review
Unusual transactional behavior	Full KYC file, transactional audit trail	Apply EDD, enhanced monitoring, report if needed
Deposit patterns inconsistent with gaming behavior	ID, SOF, device/IP log	EDD, enhanced review and justification

Annex 3 – Prohibited Jurisdictions

The following jurisdictions are classified as prohibited due to international sanctions, FATF high-risk designation, or inadequate AML/CFT controls. The Company shall not onboard or process transactions from individuals or entities linked to these jurisdictions.

- Afghanistan
- Iran
- North Korea
- Syria
- Russia
- Belarus
- Myanmar
- Albania
- Armenia
- Azerbaijan
- Barbados
- Belize
- Botswana
- Cambodia
- Ethiopia
- Ghana
- Iraq
- Israel
- Jamaica
- Kuwait
- Laos
- Mauritius
- Namibia
- Nicaragua
- Pakistan
- Panama
- Sudan
- Taiwan
- The Bahamas
- Uganda
- United States of America
- Yemen
- Zimbabwe

Annex 4 – AML Escalation Flow

This chart outlines the standard escalation path when potentially suspicious activity or non-compliant behavior is detected. All employees are obligated to report incidents through the following structured process.

Escalation Step	Responsible Function
Suspicious activity detected	Front-Office / Transaction Monitoring System
Initial Review	AML and Anti-Fraud Department
Escalation to Compliance Officer	Compliance Department
Case review and risk analysis	Compliance Officer
Decision to escalate to MLRO	CO → MLRO
STR filing decision	MLRO
goAML submission (if applicable)	MLRO
Post-filing actions / Monitoring	MLRO