

Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing Policy (AML/CFT/CPF Policy)

Board of Directors
LGE Entertainment N.V.

Responsible Office:
Compliance Department / Money Laundering Reporting Officer (MLRO)

Effective Date:
11/05/2026

Next Review Date:
11/05/2027

1. Policy Statement

LGE Entertainment N.V. ("the Company"), operating under the brand IGC BET, is committed to maintaining effective systems and controls to prevent its products, services, payment channels and platform from being used for money laundering, terrorist financing, proliferation financing, fraud, sanctions violations or any other criminal activity.

The Company adopts a risk-based approach to Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing ("AML/CFT/CPF") and is committed to complying with all applicable laws, regulations and regulatory requirements issued by the Curaçao Gaming Authority ("CGA"), the Financial Intelligence Unit Curaçao ("FIU"), and other competent authorities.

This Policy establishes the framework for identifying, assessing, monitoring, mitigating and reporting AML/CFT/CPF risks and applies to all directors, officers, employees, contractors and third-party service providers acting on behalf of the Company.

The Company maintains a zero-tolerance approach towards knowingly facilitating money laundering, terrorist financing, proliferation financing or transactions involving sanctioned individuals, entities or jurisdictions.

2. Purpose

The purpose of this Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing Policy ("Policy") is to establish a comprehensive framework for

preventing, detecting, managing and reporting activities that may involve money laundering, terrorist financing, proliferation financing, fraud, sanctions violations or other financial crimes.

This Policy is designed to:

- Ensure compliance with all applicable AML/CFT/CPF laws, regulations and regulatory requirements, including those issued by the Curaçao Gaming Authority ("CGA"), the Financial Intelligence Unit Curaçao ("FIU Curaçao"), and other competent authorities.
- Protect the Company, its customers, business partners and stakeholders from financial crime risks.
- Establish risk-based procedures for customer acceptance, customer due diligence, ongoing monitoring, sanctions screening and regulatory reporting.
- Define the roles and responsibilities of management, employees and the Money Laundering Reporting Officer ("MLRO") in maintaining an effective AML/CFT/CPF compliance framework.
- Safeguard the integrity, reputation and long-term sustainability of the Company's sportsbook, casino and gaming operations.
- Ensure that the Company maintains appropriate systems and controls to identify, assess, mitigate and monitor AML/CFT/CPF risks associated with its products, services, customers, payment methods, technologies and geographic exposure.

This Policy forms part of the Company's overall compliance and risk management framework and supports the Company's commitment to operating in a lawful, transparent and responsible manner.

3. Audience

This Policy applies to all persons involved in the management, operation and support of the Company's business activities, including:

- Directors and Shareholders.
- Senior Management.
- The Money Laundering Reporting Officer ("MLRO").
- Compliance personnel and risk management personnel.
- Customer support personnel.
- Payment, finance and operational personnel.
- Employees, whether permanent, temporary or part-time.

- Contractors, consultants and outsourced service providers engaged by the Company.
- Third-party suppliers providing services related to customer onboarding, identity verification, sanctions screening, payment processing, transaction monitoring, fraud prevention, blockchain analytics or other compliance-related functions.

All individuals and entities covered by this Policy are required to understand, comply with and support the Company's AML/CFT/CPF obligations and internal control framework.

Failure to comply with this Policy may result in disciplinary action, termination of employment or contractual relationship, regulatory reporting, and other actions deemed appropriate by the Company.

4. Definitions

For the purposes of this Policy, the following definitions shall apply:

Money Laundering (ML)

The process of concealing, disguising, transferring or converting proceeds derived from criminal activity in order to make them appear legitimate.

Terrorist Financing (TF)

The provision, collection, movement or use of funds, assets or financial services intended to support terrorist activities, terrorist organizations or individual terrorists.

Proliferation Financing (PF)

The provision of funds or financial services used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of weapons of mass destruction and related materials.

AML/CFT/CPF

Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing measures, controls and procedures.

Customer Due Diligence (CDD)

The process of identifying and verifying a customer's identity, understanding the nature and purpose of the business relationship, and assessing the associated risk.

Enhanced Due Diligence (EDD)

Additional verification, monitoring and risk mitigation measures applied to higher-risk customers, transactions or business relationships.

Politically Exposed Person (PEP)

An individual who is or has been entrusted with a prominent public function, including their immediate family members and close associates.

Source of Funds (SoF)

Information or documentation demonstrating the origin of funds used by a customer for deposits, transactions or other financial activity.

Source of Wealth (SoW)

Information or documentation demonstrating the origin of a customer's total accumulated wealth.

Sanctions

Restrictive measures imposed by the United Nations, European Union, Curaçao or other competent authorities against specific individuals, entities, countries or organizations.

Suspicious Activity

Any activity, transaction or behavior that appears unusual, inconsistent with a customer's profile, or gives rise to concerns regarding money laundering, terrorist financing, proliferation financing, fraud or other criminal conduct.

Money Laundering Reporting Officer (MLRO)

The individual appointed by the Company with responsibility for overseeing AML/CFT/CPF compliance, reviewing suspicious activity and making reports to the relevant authorities where required.

Financial Intelligence Unit (FIU Curaçao)

The competent authority responsible for receiving, analyzing and disseminating reports concerning unusual or suspicious transactions.

Risk-Based Approach (RBA)

A framework through which AML/CFT/CPF measures are applied proportionately based on the level of risk presented by customers, products, services, payment methods, jurisdictions and transactions.

Business Risk Assessment (BRA)

The documented assessment used by the Company to identify, evaluate and mitigate AML/CFT/CPF risks associated with its business activities.

Customer Risk Assessment (CRA)

The process of assessing and categorizing customer risk based on factors such as geography, payment methods, transaction activity, source of funds, sanctions exposure and other relevant indicators.

5. Policy Implementation

The Company shall implement this Policy through a risk-based AML/CFT/CPF framework designed to identify, assess, monitor, mitigate and report financial crime risks associated with its products, services, customers, payment methods, technologies and jurisdictions.

The Board of Directors and Senior Management are responsible for ensuring that adequate resources, systems and controls are maintained to support effective implementation of this Policy.

The Money Laundering Reporting Officer ("MLRO") shall be responsible for overseeing the day-to-day operation of the Company's AML/CFT/CPF compliance framework, including customer due diligence, transaction monitoring, sanctions screening, suspicious activity investigations and regulatory reporting.

The Company shall maintain documented procedures, controls and records to demonstrate compliance with applicable AML/CFT/CPF requirements and shall review such procedures periodically to ensure their continued effectiveness.

The following sections describe the key components of the Company's AML/CFT/CPF framework.

5.1 Business Risk Assessment (BRA)

The Company maintains a documented Business Risk Assessment ("BRA") designed to identify, assess, monitor and mitigate money laundering, terrorist financing and proliferation financing risks arising from its business activities.

The BRA adopts a risk-based approach and considers the risks associated with:

- Products and services;
- Customer types;
- Payment methods;
- Delivery channels;
- Geographic exposure;
- Third-party service providers;
- Technological developments.

The Company recognises that the online gaming sector may be exposed to increased ML/TF/PF risks due to the remote nature of customer onboarding, cross-border transactions, digital payment methods and online account access.

Products and Services Risk

The Company operates sportsbook, online casino and live casino products.

Potential risks include:

- Use of gambling accounts to disguise the origin of funds;
- Rapid deposits and withdrawals;
- Abuse of promotional campaigns;
- Collusion and fraudulent activity.

The Company mitigates these risks through customer due diligence, transaction monitoring, account monitoring and enhanced due diligence procedures.

Customer Risk

The Company services retail customers located in approved jurisdictions.

Higher-risk customer categories may include:

- Politically Exposed Persons (PEPs);
- Customers from higher-risk jurisdictions;
- High-value customers;
- Customers exhibiting unusual transactional behaviour.

Enhanced Due Diligence and enhanced monitoring measures are applied where appropriate.

Payment Method Risk

The Company currently supports cryptocurrency payment methods and may introduce fiat payment methods through licensed and regulated payment service providers.

Cryptocurrency transactions may present elevated risks due to the speed, global reach and pseudonymous nature of blockchain transactions.

Mitigation measures include:

- Customer verification procedures;
- Blockchain analytics and transaction monitoring tools where appropriate;
- Source of Funds reviews;
- Enhanced Due Diligence procedures;
- Ongoing transaction monitoring.

Fiat payment risks are mitigated through due diligence of payment service providers, transaction monitoring and reconciliation controls.

Delivery Channel Risk

The Company operates exclusively through remote online channels.

Risks associated with non-face-to-face onboarding are mitigated through:

- Identity verification procedures;
- Geolocation controls;
- Device monitoring;
- Ongoing customer monitoring.

Geographical Risk

The Company assesses geographic risk based on:

- Country of residence;
- Country of payment origin;
- FATF publications;
- Sanctions lists;
- Publicly available risk indicators.

Customers located in sanctioned, prohibited or otherwise unacceptable jurisdictions are not accepted.

Risk Appetite

The Company maintains a low tolerance for money laundering, terrorist financing, proliferation financing and sanctions-related risks.

The Company will not knowingly establish or maintain business relationships with:

- Sanctioned individuals or entities;
- Terrorist organisations;
- Customers providing false information;
- Customers unwilling to complete required due diligence procedures.

The Company accepts moderate operational risk associated with cryptocurrency and alternative payment methods provided that adequate controls and monitoring procedures are implemented.

Monitoring and Effectiveness

The effectiveness of AML/CFT/CPF controls is monitored through:

- Ongoing transaction monitoring;
- Internal compliance reviews;
- Management oversight;
- Regulatory reporting reviews;
- Staff training;
- Independent testing and audits where appropriate.

Identified deficiencies shall be documented, remediated and monitored until resolved.

Review and Approval

The Business Risk Assessment shall be:

- Reviewed at least annually;
- Reviewed whenever significant changes occur to products, services, payment methods, customer types, jurisdictions or regulatory requirements;
- Approved by Senior Management.

Prior to the launch of new products, business practices, delivery mechanisms, payment methods or technologies, the Company shall conduct a documented technological and AML/CFT/CPF risk assessment to identify and mitigate associated risks.

5.2 Customer Risk Assessment (CRA)

The Company applies a risk-based Customer Risk Assessment ("CRA") framework to identify, assess and manage the money laundering, terrorist financing and proliferation financing risks associated with each customer.

The CRA is conducted upon establishing a business relationship and is updated periodically throughout the customer lifecycle, or whenever significant changes occur to the customer's profile, behaviour or risk exposure.

The purpose of the CRA is to establish a customer risk profile and determine the appropriate level of due diligence, monitoring and control measures required.

The CRA is based on the risk categories identified within the Company's Business Risk Assessment ("BRA"), including:

- Customer Risk;
- Geographic Risk;
- Payment Method Risk;
- Product and Service Risk;
- Transaction Risk;
- Delivery Channel Risk.

In assessing customer risk, the Company may consider factors including:

Customer Risk Factors

- Politically Exposed Person (PEP) status;
- Adverse media findings;
- Occupation and business activities;
- Source of Funds;
- Source of Wealth where applicable;
- Previous suspicious activity indicators.

Geographic Risk Factors

- Country of residence;
- Nationality;
- Country of payment origin;
- FATF risk classifications;
- Sanctions exposure.

Payment Method Risk Factors

- Cryptocurrency transactions;

- Use of multiple payment methods;
- Third-party payment attempts;
- Future fiat payment methods and alternative payment solutions.

Transaction Risk Factors

- Volume of deposits and withdrawals;
- Frequency of transactions;
- Unusual transaction patterns;
- Transactions inconsistent with the customer's known profile.

Based on the assessment, customers shall be classified as:

Low Risk

Customers presenting limited AML/CFT/CPF risk indicators and demonstrating behaviour consistent with their profile.

Medium Risk

Customers presenting one or more elevated risk indicators requiring enhanced monitoring.

High Risk

Customers presenting significant AML/CFT/CPF risk indicators, including but not limited to PEP status, high-risk jurisdictions, adverse media findings, unusual transactional behaviour, or Source of Funds concerns.

Customers classified as High Risk shall be subject to Enhanced Due Diligence ("EDD"), increased monitoring and, where appropriate, Senior Management approval.

The Company shall review and update customer risk profiles periodically and whenever material changes occur in the customer's circumstances, transaction activity, payment methods or risk exposure.

The CRA shall be documented and retained in accordance with the Company's record-keeping requirements.

5.3 Customer Acceptance Policy (CAP)

The Company applies a risk-based Customer Acceptance Policy ("CAP") designed to ensure that customers are accepted, monitored and managed in accordance with their assessed AML/CFT/CPF risk profile.

The CAP is based on the outcome of the Customer Risk Assessment ("CRA") and determines the level of Customer Due Diligence ("CDD"), Enhanced Due Diligence ("EDD"), monitoring and approval required before and during the business relationship.

Acceptable Customers

The Company may establish and maintain a business relationship with customers who:

- Successfully complete required verification procedures;
- Provide accurate and complete information;
- Are not subject to sanctions restrictions;
- Are not associated with terrorist organisations or criminal activities;
- Reside in jurisdictions accepted by the Company;
- Present an acceptable AML/CFT/CPF risk profile.

Higher-Risk Customers

Certain customers may present higher than average AML/CFT/CPF risks and therefore require Enhanced Due Diligence ("EDD"), increased monitoring and, where appropriate, Senior Management approval.

Higher-risk customers may include:

- Politically Exposed Persons ("PEPs");
- Family members and close associates of PEPs;
- Customers residing in or connected to higher-risk jurisdictions;
- High-value customers;
- Customers using higher-risk payment methods;
- Customers exhibiting unusual transactional behaviour;
- Customers subject to adverse media findings;
- Customers where Source of Funds or Source of Wealth concerns exist;
- Customers identified through internal monitoring as presenting elevated risk.

Politically Exposed Persons (PEPs)

The Company does not automatically reject PEPs.

Prior to establishing or continuing a business relationship with a PEP, the Company shall:

- Conduct Enhanced Due Diligence;
- Establish Source of Funds;
- Establish Source of Wealth where appropriate;
- Obtain Senior Management approval;
- Apply enhanced ongoing monitoring.

Sanctions Screening

The Company shall perform sanctions screening during onboarding and periodically throughout the customer relationship.

Screening may include:

- United Nations sanctions lists;
- European Union sanctions lists;
- Other applicable sanctions lists;
- Internal watchlists where applicable.

Where a sanctions match is identified, the Company shall immediately restrict the account, investigate the match and take any action required by applicable laws and regulations.

Unacceptable Customers

The Company shall refuse, restrict or terminate relationships with customers who:

- Appear on applicable sanctions lists;
- Are linked to terrorist organisations or terrorist financing;
- Provide false, misleading or incomplete information;
- Submit forged, altered or fraudulent documentation;
- Refuse to complete required due diligence procedures;
- Refuse to provide Source of Funds or Source of Wealth information when required;
- Attempt to circumvent geographic restrictions;
- Are reasonably suspected of engaging in money laundering, terrorist financing, proliferation financing, fraud or other criminal activity;
- Present a level of risk that exceeds the Company's risk appetite.

The Company reserves the right to refuse, restrict or terminate any business relationship where it is unable to effectively manage the associated AML/CFT/CPF risks.

The rationale for all high-risk customer approvals, refusals and terminations shall be documented and retained in accordance with the Company's record-keeping requirements.

5.4 Customer Due Diligence (CDD)

The Company applies risk-based Customer Due Diligence ("CDD") measures to identify and verify customers, understand the nature and purpose of the business relationship, and assess the associated AML/CFT/CPF risks.

CDD measures shall be performed:

- Prior to establishing a business relationship where required;
- Upon reaching applicable regulatory thresholds;
- When suspicious activity is identified;
- When customer information changes materially;
- When doubts arise regarding the accuracy or adequacy of previously obtained information.

Customer Identification and Verification

The Company may collect and verify information including:

- Full legal name;
- Date of birth;
- Residential address;
- Nationality;
- Government-issued identification document;
- Contact information;
- Source of Funds information where required;
- Source of Wealth information where required.

Identity verification may be performed through internal procedures and/or independent third-party verification providers.

PEP Screening

Customers shall be screened for Politically Exposed Person ("PEP") status during onboarding and periodically throughout the business relationship.

Where a customer is identified as a PEP, the Company shall:

- Conduct Enhanced Due Diligence;
- Establish Source of Funds;
- Establish Source of Wealth where appropriate;
- Obtain Senior Management approval;
- Apply enhanced ongoing monitoring.

Sanctions Screening

The Company shall conduct sanctions screening against applicable United Nations and European Union sanctions lists:

- During onboarding;
- On a periodic ongoing basis, at least monthly;
- Upon material changes to customer information;
- Prior to processing transactions where deemed necessary based on risk.

Where a sanctions match is identified:

- The customer account shall be immediately restricted;
- Any funds shall be frozen where required by applicable laws and regulations;
- The MLRO shall investigate the match;
- The Company shall submit reports and notifications to the competent authorities in Curaçao where required by law;
- The account shall remain restricted until the matter is resolved.

XCG 4,000 Threshold

Where a customer reaches the cumulative threshold of XCG 4,000 and the required due diligence documentation has not been completed, the Company shall:

- Suspend further deposits;
- Restrict withdrawals;
- Request outstanding verification documents;
- Notify the customer of the verification requirement.

The customer shall be granted a period of up to thirty (30) days to provide the requested information and documentation.

Failure to Provide Information Within 30 Days

Where the required documentation is not provided within thirty (30) days of reaching the XCG 4,000 threshold:

- The business relationship shall be reviewed and may be terminated;
- Deposits and withdrawals shall remain restricted;
- The business relationship shall be reviewed by the MLRO and Compliance function;
- Appropriate risk mitigation measures shall be applied.

Termination of Business Relationship

The Company may terminate a business relationship where:

- Required due diligence information is not provided;
- Verification cannot be satisfactorily completed;
- False or misleading information is identified;
- The customer presents unacceptable AML/CFT/CPF risks;
- Regulatory requirements prohibit continuation of the relationship.

Prior to termination, the Company shall document the reasons for the decision, consider any reporting obligations and determine whether funds may be returned, frozen or otherwise handled in accordance with applicable laws and regulatory requirements.

All decisions relating to account restrictions, suspensions, terminations and regulatory reporting shall be documented and retained in accordance with the Company's record-keeping requirements.

5.5 Ongoing Monitoring

The Company conducts ongoing monitoring throughout the customer relationship to ensure that customer activity remains consistent with the Company's knowledge of the customer, the customer's risk profile, source of funds and expected behaviour.

The purpose of ongoing monitoring is to identify unusual, suspicious or potentially high-risk activity that may indicate money laundering, terrorist financing, proliferation financing, fraud or other criminal conduct.

Customer Identity Monitoring

The Company shall periodically review customer information to ensure that identification and verification records remain accurate, complete and up to date.

The Company may request updated information or documentation where:

- Customer information changes;
- Identification documents expire;
- Risk profiles change;
- Suspicious activity is identified;
- Additional regulatory requirements apply.

The Company may re-verify customer identity where appropriate.

Transaction Monitoring

The Company monitors customer transactions and account activity using a risk-based approach.

Monitoring may include:

- Deposit activity;
- Withdrawal activity;
- Transaction volumes;
- Transaction frequency;
- Payment methods used;
- Gameplay activity;
- Account access patterns;
- Device and geolocation information;
- Source of Funds information where appropriate.

The Company may utilise automated monitoring systems, blockchain analytics tools, fraud prevention systems and manual reviews to identify unusual or suspicious activity.

Red Flag Indicators

Examples of activity that may trigger additional review include:

- Rapid deposits and withdrawals with limited gameplay;
- Transaction activity inconsistent with the customer's known profile;
- Significant increases in transaction volume;

- Use of multiple payment methods without reasonable explanation;
- Attempts to circumvent verification requirements;
- Use of technologies designed to conceal location or identity;
- Activity associated with high-risk jurisdictions;
- Potential account sharing or multiple account activity.

Enhanced Monitoring

Where a customer is classified as High Risk or where suspicious indicators are identified, the Company may apply Enhanced Monitoring measures, including:

- Increased transaction review;
- Additional verification requests;
- Source of Funds reviews;
- Source of Wealth reviews;
- Enhanced Due Diligence procedures;
- Escalation to the MLRO.

Monitoring Outcomes

Where ongoing monitoring identifies unusual or suspicious activity, the Company may:

- Request additional information or documentation;
- Restrict account activity;
- Apply Enhanced Due Diligence;
- Escalate the matter to the MLRO;
- Submit reports to competent authorities where required;
- Terminate the business relationship where appropriate.

All monitoring activities, reviews, investigations and decisions shall be documented and retained in accordance with the Company's record-keeping requirements.

5.6 Reliance on Third Parties to Perform Customer Due Diligence

The Company may utilise appropriately qualified and reputable third-party service providers to assist in the performance of Customer Due Diligence ("CDD"), Enhanced Due Diligence ("EDD"), sanctions screening, identity verification, address verification, fraud prevention, transaction monitoring and blockchain analytics activities.

Such third-party providers may include identity verification providers, sanctions screening providers, compliance technology providers, payment service providers and other regulated service providers.

Prior to engaging a third-party provider, the Company shall conduct appropriate due diligence to ensure that the provider possesses the necessary expertise, systems, controls and compliance standards required to support the Company's AML/CFT/CPF obligations.

Where reliance is placed on a third party, the Company shall ensure that:

- Relevant customer information can be obtained without undue delay;
- Appropriate records are maintained;
- The third party is subject to appropriate regulatory oversight or equivalent controls where applicable;
- The effectiveness of the provider is periodically reviewed.

The Company remains ultimately responsible for compliance with all AML/CFT/CPF obligations and shall not transfer or delegate its legal and regulatory responsibilities to any third party.

The MLRO and Compliance function shall oversee all arrangements involving reliance on third parties and shall periodically assess their effectiveness and suitability.

5.7 Reporting of Unusual Transactions

The Company maintains procedures to identify, investigate, document and report unusual or suspicious transactions in accordance with applicable AML/CFT/CPF laws, regulations and regulatory requirements.

All employees, contractors and service providers acting on behalf of the Company are required to promptly report any unusual or suspicious activity to the Money Laundering Reporting Officer ("MLRO").

Identification of Unusual Transactions

The Company may identify unusual transactions through:

- Customer Due Diligence reviews;
- Ongoing transaction monitoring;
- Enhanced Due Diligence procedures;
- Sanctions screening;
- Fraud monitoring systems;
- Internal alerts and investigations;
- Employee observations and escalations.

Indicators of unusual activity may include, but are not limited to:

- Transactions inconsistent with the customer's known profile;
- Rapid deposits and withdrawals with limited gameplay;
- Structuring transactions to avoid regulatory thresholds;
- Use of multiple payment methods without reasonable explanation;
- Unusual account activity;
- Source of Funds concerns;
- Activity involving high-risk jurisdictions.

XCG 5,000 Reporting Threshold

Where an unusual transaction is identified and the applicable every transaction above XCG 5,000 is reported, the matter shall be immediately escalated to the MLRO for review.

The MLRO shall:

- Assess the available information;
- Conduct further investigation where appropriate;
- Document the findings;
- Determine whether a report must be submitted to the Financial Intelligence Unit Curaçao ("FIU Curaçao").

Where required by law, the Company shall submit the relevant report to FIU Curaçao without undue delay.

Internal Reporting and Escalation

All internal reports and investigations shall be documented and retained.

The MLRO shall maintain records of:

- Internal suspicious activity reports;
- Investigations conducted;
- Decisions made;
- Reports submitted to competent authorities;
- Supporting documentation and evidence.

Prohibition of Tipping-Off

Employees, contractors and service providers are strictly prohibited from informing any customer or third party that:

- A report has been submitted to FIU Curaçao;
- An investigation is being conducted;
- Regulatory authorities have been notified;
- The customer's activity is under review.

Any unauthorised disclosure may result in disciplinary action and may constitute a breach of applicable AML/CFT/CPF laws and regulations.

Record Keeping

The Company shall maintain and retain records relating to:

- Customer identification and verification information;
- Customer Risk Assessments;

- Customer Due Diligence and Enhanced Due Diligence records;
- Source of Funds and Source of Wealth documentation;
- Transaction records;
- Payment records;
- Internal investigation records;
- Regulatory reporting records.

Records shall be retained for a minimum period of five (5) years following the end of the business relationship or the completion of the relevant transaction, whichever is later.

Records shall be stored securely and shall be made available to competent authorities upon lawful request.

5.8 Anti-Money Laundering Compliance Program

The Company maintains a risk-based Anti-Money Laundering, Counter-Terrorist Financing and Counter-Proliferation Financing ("AML/CFT/CPF") Compliance Program designed to identify, assess, mitigate, monitor and report financial crime risks associated with its products, services, customers, payment methods, technologies and jurisdictions.

The AML Compliance Program is designed to establish minimum standards reasonably intended to ensure compliance with applicable laws, regulations and regulatory requirements, including those issued by the Curaçao Gaming Authority ("CGA"), the Financial Intelligence Unit Curaçao ("FIU Curaçao") and other competent authorities.

The AML Compliance Program includes the following components:

Governance and Oversight

- Board and Senior Management oversight of AML/CFT/CPF risks;
- Appointment of a qualified Money Laundering Reporting Officer ("MLRO");
- Allocation of adequate resources to support compliance activities;
- Periodic review of AML/CFT/CPF controls and procedures.

Risk-Based Approach

- Business Risk Assessments ("BRA");
- Customer Risk Assessments ("CRA");
- Customer Acceptance Policy ("CAP");
- Ongoing review of risk exposure;
- Periodic reassessment of emerging risks.

Customer Due Diligence

- Customer identification and verification;
- Enhanced Due Diligence procedures;

- Source of Funds and Source of Wealth reviews where required;
- Politically Exposed Person ("PEP") screening;
- Sanctions screening.

Ongoing Monitoring

- Transaction monitoring;
- Customer activity monitoring;
- Enhanced monitoring of higher-risk customers;
- Investigation of unusual or suspicious activity;
- Regulatory reporting where required.

Policies, Procedures and Internal Controls

- Written AML/CFT/CPF policies and procedures;
- Internal reporting procedures;
- Escalation procedures;
- Record retention procedures;
- Compliance controls and monitoring mechanisms.

Training and Awareness

The Company shall provide AML/CFT/CPF training to relevant personnel on a periodic basis.

Training may include:

- AML/CFT/CPF obligations;
- Customer Due Diligence procedures;
- Customer Acceptance Policy requirements;
- Identification of suspicious activity;
- Reporting obligations;
- Record-keeping requirements;
- Regulatory developments.

Training records shall be maintained and retained.

Independent Review and Testing

The Company shall periodically assess the effectiveness of its AML/CFT/CPF framework through internal reviews, compliance testing and, where appropriate, independent assessments.

Any deficiencies identified shall be documented, addressed and monitored until remediation has been completed.

Record Keeping

The Company shall maintain records relating to:

- Customer Due Diligence;
- Risk assessments;
- Monitoring activities;
- Investigations;
- Regulatory reporting;
- Employee training.

Records shall be retained in accordance with applicable legal and regulatory requirements.

Continuous Improvement

The Company shall review and update its AML/CFT/CPF Compliance Program whenever significant changes occur to:

- Products or services;
- Payment methods;
- Customer types;
- Geographic exposure;
- Regulatory requirements;
- Technologies or delivery channels.

In the absence of material changes, the AML Compliance Program shall be reviewed at least annually to ensure its continued effectiveness and compliance with applicable laws and regulations.

6. Compliance and Consequences of Non-Compliance

Compliance with this Policy is mandatory for all directors, officers, employees, contractors, consultants and third-party service providers acting on behalf of the Company.

All persons subject to this Policy are responsible for understanding and complying with the Company's AML/CFT/CPF obligations and for promptly reporting any actual, suspected or potential violations.

Failure to comply with this Policy may expose the Company to significant regulatory, legal, financial and reputational risks, including:

- Regulatory sanctions and enforcement actions;
- Financial penalties and fines;
- Suspension or revocation of licences and approvals;
- Civil liability;
- Criminal prosecution;
- Reputational damage;
- Loss of business opportunities and commercial relationships.

Where a breach of this Policy is identified, the Company may take appropriate corrective and disciplinary action, including:

- Additional training and supervision;
- Formal warnings;
- Restriction of duties or responsibilities;
- Suspension from employment or engagement;
- Termination of employment, contract or business relationship;
- Reporting to regulatory, law enforcement or other competent authorities where required.

Employees and service providers are required to cooperate fully with internal investigations, compliance reviews and regulatory inquiries.

No employee, officer or service provider shall suffer retaliation for reporting concerns, suspicious activity or potential violations of this Policy in good faith.

The Company is committed to maintaining a strong culture of compliance and expects all personnel to act with integrity, transparency and professionalism in fulfilling their AML/CFT/CPF responsibilities.

7. Related Information

This Policy should be read in conjunction with the following internal policies, procedures, legal requirements and regulatory guidance documents:

Internal Policies and Procedures

- Business Risk Assessment (BRA)
- Customer Risk Assessment (CRA)
- Customer Acceptance Policy (CAP)
- Customer Verification and Identification Procedures
- Sanctions Screening Procedures
- Politically Exposed Persons (PEP) Procedures
- Record Retention Policy
- Responsible Gambling Policy
- Data Protection and Privacy Policy
- Information Security Policy

- Incident Management Procedures
- Employee Code of Conduct

Legal and Regulatory Framework

- National Ordinance on the Prevention and Combating of Money Laundering and Terrorist Financing (Curacao)
- Regulations for the Combating of Money Laundering and Financing of Terrorism issued by the Curaçao Gaming Authority
- Applicable Sanctions Legislation and Regulations
- Applicable Financial Intelligence Unit Curaçao (FIU Curaçao) Guidance
- Applicable Curaçao Gaming Authority (CGA) Directives, Guidance and Regulatory Requirements

International Standards and Guidance

- Financial Action Task Force (FATF) Recommendations
- FATF Risk-Based Approach Guidance
- United Nations Security Council Sanctions Resolutions
- European Union Restrictive Measures and Sanctions Framework

The Company shall review and update references contained in this section whenever material changes occur to applicable laws, regulations, guidance or internal procedures.

8. Contact Information

For any questions regarding this Policy or the Company's AML/CFT/CPF compliance framework, please contact:

Money Laundering Reporting Officer (MLRO)

LGE Entertainment N.V.

Name: Elvin Cani

Position: Compliance Officer

Email: elvincani@gmail.com

Telephone: +355 69 601 2038

Registered Address: Babej Street, 4001

The MLRO is responsible for overseeing the Company's AML/CFT/CPF compliance program, receiving internal reports of suspicious activity, liaising with competent authorities and providing guidance regarding AML/CFT/CPF obligations.

9. Policy History

This Policy shall be reviewed at least annually and updated whenever material changes occur to the Company's business activities, products, services, payment methods, customer base, regulatory obligations or risk profile.

Any future revisions shall be documented and approved by Senior Management prior to implementation.



(SMES) Solutions for Management and Employment Support N.V.

Managing Director

16.06.2026