Know Your Customer (KYC), Anti-Money Laundering (AML), Countering the Financing of Terrorism (CTF) and Proliferation Financing (PF) Policy

MCG Technologies N.V.

Table of Contents

Version Control

Version	Date	Author	Comments
1.0	12 June 2026	Compliance Officer	First Version – new company acquisition

1. Purpose

MCG Technologies N.V. (the “Operator”, “Company”, “us”, “we”) operates online gaming services under the CGA licence. The primary purpose of this policy is to prevent the Company from being used for money laundering (ML), terrorist financing (TF), proliferation financing (PF), or other illicit financial activities.

It establishes a comprehensive, risk-based AML/CTF program that:

- Identifies, assesses, and mitigates ML/TF/PF risks specific to online/remote gaming.
- Implements robust customer identification, verification, due diligence, monitoring, and reporting mechanisms.
- Ensures compliance with Curaçao law, CGA regulations, and international standards (FATF).
- Protects the integrity of gaming operations, player funds, the Company’s reputation, and Curaçao’s jurisdiction.
- Promotes a culture of compliance through governance, training, independent oversight, and continuous improvement.

The Company applies a zero-tolerance approach towards money laundering, terrorist financing and proliferation financing. Failure to comply with this policy may result in disciplinary action, including termination of employment.

2. Scope

This policy applies to:

- All Company activities, including player onboarding, deposits, wagers, withdrawals, transfers between accounts, bonuses, and any financial transactions.
- All employees, contractors, third-party providers (payment processors, affiliates, software suppliers), and agents.
- All players, including existing and prospective players.
- All delivery channels.
- All products and services offered by us.

3. Regulatory Context

This policy fully implements and complies with Curaçao's AML/CTF framework for licensed gaming operators:

- **Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction** (Version January 10, 2025) issued by the Curaçao Gaming Authority (CGA):

https://gamingcontrol.spin-cdn.com/media/aml_cft/20250110_regulations_for_the_combating_of_money_laundering_and_financing_of_terrorism_version_january_10_2025.pdf

- National Ordinance on Identification when Rendering Services (LID) and National Ordinance on the Reporting of Unusual Transactions (LMOT)
- National Ordinance on Games of Chance (LOK) (PB 2024, no. 157, effective December 24, 2024): https://gamingcontrol.spin-cdn.com/media/online_gaming/20241230_landsverordening_op_de_kansspelen.pdf
- Alignment with FATF Recommendations, National Risk Assessments, UN/EU/Curaçao sanctions lists, and Kingdom Sanctions Act.

4. Definitions

- **Money Laundering (ML)**: Process of disguising illicit funds as legitimate (placement, layering, integration).
- **Terrorist Financing (TF)**: Providing/supporting funds or assets for terrorist acts/organisations.
- **Proliferation Financing (PF)**: Financing weapons of mass destruction programs.
- **Unusual Transaction**: Any transaction or pattern inconsistent with player profile, business purpose, or risk level (for example, transaction over NAf 5,000 equivalent or complex/large without economic rationale).
- **Customer Due Diligence (CDD)**: Standard identification/verification and ongoing monitoring.
- **Enhanced Due Diligence (EDD)**: Additional measures for high-risk scenarios.
- **Simplified Due Diligence (SDD)**: Reduced measures for verifiable low-risk cases (not permitted if suspicion exists).
- **Politically Exposed Person (PEP)**: Domestic/foreign individuals entrusted with prominent public functions, family members, close associates.
- **Beneficial Owner**: Natural person(s) ultimately owning/controlling ≥25% or exercising control over the customer (or on whose behalf playing occurs).

- **goAML**: FIU Curaçao's secure portal for reporting unusual/suspicious transactions.

5. Risk-based Approach

5.1 Business Risk Assessment (BRA)

The Company conducts an enterprise-wide Business Risk Assessment (BRA) to identify, analyse, and evaluate all ML/TF/PF risks to which its online gaming operations are exposed. The BRA forms the foundation of the entire AML/CFT/PF program and ensures that all policies, procedures, controls, and resources are proportionate to the actual risks faced.

5.1.1 Purpose and Scope of the BRA

The BRA assesses the ways in which the Company's products, services, delivery channels, and customer base could be exploited for money laundering, terrorist financing, or proliferation financing. It takes into account the outcomes and recommendations of Curaçao's National Risk Assessment (NRA) and any relevant sector-specific guidance issued by the CGA.

5.1.2 Four Core Risk Categories Assessed

The BRA explicitly covers the following gambling-sector-specific risk areas:

1. **Customer Risk**
    - Customers with multiple or irregular income streams
    - Politically Exposed Persons (PEPs)
    - High spenders or disproportionate spenders (inconsistent with known source of income/wealth)
    - Third-party play, syndicates, junkets, or attempts at the use of multiple accounts.

2. **Geographical Risk**
    - Nationality, residence, or place of birth of players
    - High-risk jurisdictions (FATF High-Risk Jurisdictions subject to a Call for Action, FATF Jurisdictions under Increased Monitoring, CFATF Public Statement, European Commission strategic deficiencies list, OFAC-sanctioned countries, countries identified as providing funding/support for terrorism, or high-corruption countries per Transparency International Corruption Perceptions Index)
    - The Company maintains and regularly updates an internal High-Risk Country List.

3. **Product, Service and Transaction Risk**

    - Anonymous or high-risk payment methods (crypto, e-wallets accepting cash, prepaid cards)
    - Minimal or no-play activity followed by large withdrawals
    - Peer-to-peer fund transfers between accounts
    - Use of third-party accounts/cards
    - Specific games allowing even bets or player influence (e.g., roulette, craps)
    - Multiple casino accounts or wallets under the same brand.

4. **Distribution Channel Risk**

    - Non-face-to-face onboarding and transactions (website/mobile app)
    - Involvement of third parties (affiliates, payment providers)

5.1.3 Technological Developments Risk Assessment

Before launching any new product, business practice, delivery mechanism, or technology (or material changes to existing ones), a separate documented risk assessment is performed to identify whether the innovation could create new ML/TF/PF vulnerabilities. Risks are mitigated prior to launch.

5.1.4 Methodology, Documentation and Approval

- The BRA uses a documented methodology that includes risk scoring (low/medium/high), weighting of factors, and data sources (internal transaction data, external intelligence, CGA guidance, FATF/CFATF reports).

- It records:
    - the methodology adopted;
    - reasons for classifying each risk factor as low, medium or high;
    - the overall outcome of the BRA; and
    - all information sources used.

- The BRA sets the Company's risk appetite and directly feeds into the Customer Acceptance Policy (CAP).

- The BRA is formally approved by the Board of Directors.

- It is reviewed at least annually, or immediately upon material changes (new payment methods, new markets, new games, regulatory updates, or significant

incidents).

- The full BRA document (including all supporting analysis) is made available to the Curaçao Gaming Authority (CGA) upon request and is stored securely for audit purposes.

5.1.5 Risk Appetite and Mitigation

Following the BRA, the Company defines its acceptable level of risk and implements targeted controls (e.g., enhanced monitoring for high-risk categories, automated alerts, blockchain analytics for crypto). Residual risks are documented and regularly monitored for effectiveness.

5.1.6 Money Launderging Reporting Officer

The MLRO is responsible for maintaining the BRA and ensuring its implementation. Where identified risks exceed the Company's defined risk appetite, the MLRO shall:

- Escalate the matter to senior management;
- Propose mitigating measures;
- Document all decisions and actions taken.

The MLRO operates independently from operational functions and has unrestricted access to all relevant data. The MLRO has the authority to:

- Block transactions;
- Escalate issues directly to senior management;
- Submit reports to the FIU without prior approval.

5.2 Customer Risk Assessment (CRA) & Customer Acceptance Policy (CAP)

The Company performs a Customer Risk Assessment (CRA) for every player to evaluate the specific ML/TF/PF risks posed by that individual (or legal entity) when entering into a business relationship or carrying out an occasional transaction.

It is revised on an ongoing basis whenever there is a material change in the player's behaviour, transaction pattern, risk indicators, or when new information becomes available (e.g., change of address, payment method, or sudden increase in activity).

5.2.1 Purpose of the CRA

The CRA builds a detailed customer risk profile by analysing the player's:

- Economic activity and source of wealth/income
- Transaction patterns and expected activity level
- Geographical factors

- Payment methods used
- Any red-flag indicators.

This profile determines the appropriate level of Customer Due Diligence (CDD), ongoing monitoring, and controls to be applied.

5.2.2 Customer Acceptance Policy (CAP)

The CRA directly feeds into the Company's formal Customer Acceptance Policy (CAP), which is approved by the Board and reviewed annually.

The CAP clearly defines:

- Types of players likely to pose a higher-than-average risk of ML/TF/PF (e.g., PEPs, disproportionate spenders, third-party players).
- Risk indicators that classify a player as low, medium, or high risk.
- The exact level of CDD measures (standard, enhanced, or simplified) and ongoing monitoring to be applied for each risk category.
- Circumstances under which the Company will decline to onboard or continue a relationship (e.g., inability to verify identity, sanctions hit, unresolvable high risk, or refusal to provide source-of-wealth information).

The CAP explicitly incorporates the Company's obligations regarding Politically Exposed Persons (PEPs) and sanctions screening. Senior management (or MLRO) approval is required before accepting or continuing any high-risk relationships.

All customer acceptance and rejection decisions shall be documented. High-risk customer onboarding requires:

- Review by the Compliance Officer or MLRO;
- Formal approval by senior management.

Where a customer is rejected, the reasons shall be documented and retained for audit purposes.

5.2.3 Risk Rating Categories

- Low risk: Stable profile, transparent source of funds, low-value regular activity, low-risk jurisdiction – reviewed within 5 business days.
- Medium risk: Moderate deviations or higher-risk payment methods that can be mitigated – reviewed within 3 business days.
- High risk: PEPs, disproportionate spending, anonymous/high-risk payments, high-risk jurisdictions, or multiple red flags – reviewed within 24 hours.

All CRA outcomes, supporting rationale, and risk-rating decisions are fully documented and stored for at least five years.

6. KYC Procedure

6.1 When KYC/CDD is Required

- At account opening (minimum identification).
- When financial transactions (deposits/withdrawals/transfers) reach or exceed NAf 4,000 (cumulative daily; linked transactions in same session counted).
- Occasional transactions ≥ NAf 4,000.
- Suspicion of ML/TF/PF or doubts on prior data obtained from the customer.
- Before withdrawals that would trigger the threshold.

6.2 Minimum Identification Information

At account opening (even if low-risk):

- Full name
- Permanent residential address
- Date of birth

Low-risk scenarios may limit to these three; high-risk requires additional (place of birth, nationality, identity number, occupation, source of wealth).

6.3 Verification of Identity

- Government-issued photo ID (passport, national ID, driver's licence – clear, valid, unexpired, screenshots are not allowed).
- Proof of address (for example, utility bill or bank statement issued less than 6 months, fixed-line phone bills accepted).
- Additional methods that may be adopted depnding on the risk level presented by the player: biometric/selfie match, video call, geolocation/IP/device fingerprinting, verification code to verified email/phone, social media/public databases.
- All documents must be clear, legible, and authentic.

6.4 Termination of the Business Relationship

If the Company is unable to complete the required Customer Due Diligence (CDD) measures set out in Section III.2 of the CGA Regulations (January 2025), it terminates the business relationship with the player.

Where the NAf 4,000 threshold is reached, the customer must complete full CDD within 30 days. If CDD is not completed within this timeframe:

- The account shall be blocked;
- The business relationship shall be terminated;

- The transaction shall be assessed for potential reporting to the FIU.

6.4.1 Actions upon Termination

- The Company immediately closes or blocks/suspends the player's gaming account in its entirety.
- The Company maintains a complete, dated record of all attempts made to obtain the necessary CDD information and documentation from the player (including dates of requests, methods of communication, and the player's responses or lack thereof). These records are retained for at least five years.

6.4.2 Post-Termination Review

If the player subsequently provides the requested information and/or documentation after the account has been closed or blocked/suspended, the Company:

- Assesses whether the delay in providing the CDD documentation affects the overall ML/TF/PF risk associated with the former business relationship.
- Evaluates all available factors and information to determine whether there are grounds giving rise to a suspicion of ML/TF/PF.

It is noted that mere reluctance or failure by the player to provide CDD information on its own must not be automatically treated as suspicion of ML/TF/PF. The Company considers the full context, including the player's previous behaviour, transaction history, and any other red-flag indicators before reaching a conclusion.

6.4.3 Reporting Obligation

If, after the above review, there is a presumption that the transaction or relationship is related to money laundering, terrorist financing, or proliferation financing, the Company files an Unusual Transaction Report (UTR) to the FIU via the goAML portal.

Employees must report unusual transactions immediately to the MLRO. The MLRO shall determine whether external reporting is required and submit the report to the FIU without delay. All decisions (reporting or non-reporting) must be documented and justified.

6.4.4 Return of Funds

Where there is no reason to retain the funds (i.e., no suspicion of ML/TF/PF or legal requirement to freeze), the funds must be remitted back to the player through the same channel(s) used to receive the original deposits. The Company documents the refund transaction fully.

7. Sanctions and PEPs Screening

7.1 Sanction Screening

All players (and beneficial owners where applicable) are screened against current sanctions lists:

- United Nations Security Council Consolidated List: https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list
- European Union Sanctions Map: https://www.sanctionsmap.eu/#/main
- Any local Curaçao sanctions lists published by the Curaçao Gaming Authority (CGA/GCB) or published in the National Gazette.
- Additional lists as required (e.g., OFAC where relevant for risk mitigation).

The Company subscribes to real-time sanctions database feeds and conducts manual verification of any automated hits. Sanctions Decrees and Regulations are checked for amendments on a regular basis (at least monthly) and the screening lists/systems are updated immediately. All screening results and actions are documented.

Where a customer is identified as a sanctioned person or entity:

- All funds must be frozen immediately without prior notice;
- The MLRO must be notified immediately;
- A report must be submitted to the FIU;
- No transactions shall be permitted on the account.

7.2 PEP Screening and Enhanced Measures

The Company determines whether a customer or beneficial owner is a Politically Exposed Person (PEP) using reliable, independent sources. PEP screening covers:

- Foreign PEPs (entrusted with prominent public functions abroad).
- Domestic PEPs (prominent public functions in Curaçao or the Kingdom).
- International organisation PEPs (entrusted with prominent functions by an international organisation).
- Family members and close associates of any of the above.

7.2.1 Screening timing and frequency:

- At onboarding (as part of initial CDD).
- Ongoing (regular automated and manual screening throughout the business relationship).
- Whenever a player who was not previously a PEP becomes one, the Company implements required measures within 30 days of becoming aware. Failure to do so results in termination of the relationship.

7.2.2 PEP Screening Sources:

- Public databases and internet searches.
- knowyourcountry.com
- Transparency International Corruption Perceptions Index and reports.
- PEP Caribbean list (for local PEPs).
- Adverse media screening and specialised PEP databases.

7.2.3 Enhanced Due Diligence and Measures for PEPs:

Where a PEP (or family member/close associate) is identified:

- Appropriate risk-management systems are in place to determine PEP status (already covered above).
- Senior management approval (MLRO or Compliance Department Manager) is obtained before establishing, continuing, or conducting an occasional transaction with the PEP.
- Reasonable measures are taken to establish the source of wealth and source of funds**.** The player must provide a statement, which is then verified against independent, reliable sources (public records, bank statements, payslips, inheritance documents, etc.). Public sources are used first and additional documentation is requested where necessary.
- Enhanced ongoing monitoring of the business relationship and transactions is applied, including but not limited to, increased frequency of monitoring, lower monitoring alert thresholds and senior manager review of activity.

The level of measures is tailored to the specific risk of the PEP, focussing on the type of public function, country of origin, nature of transactions. All PEP decisions, approvals, source-of-wealth verifications, and enhanced monitoring records are documented and retained for at least five years.

8. Transaction Monitoring & Red Flags

The Company operates a comprehensive, risk-based transaction monitoring programme to detect, investigate and report activity that may indicate money laundering (ML), terrorist financing (TF), proliferation financing (PF), or other financial crime. This programme forms an integral part of the ongoing Customer Due Diligence (CDD) obligation (Regulations III.2.4) and directly supports the reporting of unusual transactions (Regulations IV).

8.1 Purpose and Legal Basis

Transaction monitoring ensures that all deposits, wagers, withdrawals, transfers, bonuses, and peer-to-peer movements are consistent with the player's documented risk profile, source of wealth/funds, expected activity level and the overall Business Risk

Assessment (BRA). Any deviation triggers investigation and, where necessary, an Unusual Transaction Report (UTR) to the FIU via goAML.

8.2 Monitoring System

The Company applies a combination of automated and manual monitoring proportionate to the player's risk rating (low/medium/high) as determined by the Customer Risk Assessment (CRA):

- **Automated monitoring** – Real-time and periodic rules-based system that flags predefined thresholds and patterns.
- **Manual review** – All automated alerts are investigated by the MLRO or designated compliance analysts. High-risk or complex alerts receive senior management/MLRO oversight.
- **Frequency** – Continuous for high-risk players, periodic for medium-risk, and basic oversight for low-risk.

Monitoring covers every financial movement and non-financial indicator (e.g., login patterns, session duration, game selection) that may signal unusual behaviour.

All transaction monitoring alerts are reviewed within the following timeframes:

- High-risk alerts: within 24 hours;
- Medium-risk alerts: within 3 business days;
- Low-risk alerts: within 5 business days.

The MLRO is responsible for oversight of all high-risk alerts.

8.3 Red Flags and Indicators

The Company uses the full set of gambling-sector-specific risk factors (Regulations II.2.3) plus the objective and subjective indicators in the Ministerial Decree on Unusual Transactions. Red flags are grouped by category for operational clarity and are embedded in the automated system.

1. Customer Risk Red Flags

- Multiple or irregular sources of income inconsistent with declared profile.
- Politically Exposed Persons (PEPs) or close associates.
- High or disproportionate spending relative to known wealth/income.
- Use of third parties to deposit, wager or withdraw.
- Multiple player accounts used to fragment activity or evade tracking.

2. Geographical Risk Red Flags

- Player from, or funds sourced from, high-risk jurisdictions (FATF high-risk/grey list, sanctioned countries, high-corruption jurisdictions – see Company's maintained High-Risk Country List).
- Frequent transfers to or from high-risk countries.

3. Product, Service and Transaction Risk Red Flags

- Proceeds potentially linked to crime (check fraud, card fraud, narcotics, theft).
- Use of anonymous/high-risk payment methods (crypto, prepaid cards, e-wallets accepting cash).
- Deposit and immediate withdrawal (or minimal/no play) – "in-and-out" or "parking" behaviour.
- Rapid cycling of funds (high-velocity deposits/withdrawals with little wagering).
- Structuring (multiple transactions just below NAf 4,000 / NAf 5,000 thresholds).
- Peer-to-peer transfers or fund movements between accounts.
- Use of third-party accounts or cards.
- Even-bet games (e.g., roulette, craps) with unusually large or patterned stakes.
- Multiple casino accounts/wallets under the same operator.
- Identity fraud indicators (stolen details, mismatched geolocation/device).

4. Distribution Channel Risk Red Flags

- Non-face-to-face activity without adequate technological mitigation (e.g., no biometrics or device fingerprinting).
- Involvement of unregulated third parties (physical establishments, affiliates, payment providers).

5. Additional Objective Indicators

- Any transaction (single or linked series) ≥ NAf 5,000 (cashless transfers, deposits, cash-outs, credit-card/e-wallet transactions).
- Transactions linked to sanctioned persons/entities.
- Any transaction reported to Police or Department of Justice in connection with ML/TF.

6. Subjective/Presumed Indicators

Any pattern that appears to have no apparent economic or lawful purpose, or deviates materially from the player's established profile.

8.4 Investigation and Escalation

- Every alert is logged and investigated promptly.
- The MLRO reviews all high-risk alerts.
- If the activity cannot be explained to the Company's satisfaction, it is classified as an unusual transaction and reported to the FIU via goAML without delay.

- No tipping-off is permitted - the player is not informed of the investigation or report. Under no circumstances shall any employee disclose to a customer or third party that a report has been made or that an investigation is underway. Any breach of this requirement constitutes a serious compliance violation.

8.5 Record Keeping

AML/CFT-related records, including CDD data, transaction records, monitoring logs, and UTR documentation, shall be retained for a minimum of five (5) years. Records are readily available for inspection by the CGA and FIU.

8.6 Integration with Other Controls

Transaction monitoring results feed back into the CRA (possible risk re-rating), trigger Enhanced Due Diligence (EDD) where needed, and support the annual BRA review. Staff receive specific training on recognising these red flags.

9. Employee Screening & Training

The Company maintains a robust employee screening programme and an ongoing employee training programme to ensure that all staff possess the knowledge, skills and integrity required to prevent, detect and report money laundering, terrorist financing and proliferation financing. These programmes are mandatory, documented and form an integral part of the overall AML/CFT/PF Compliance Programme.

9.1 Employee Screening Programme

All employees, contractors, temporary staff and third-party service providers who may have access to player data, financial transactions or compliance processes are subject to screening before they commence work and on a periodic basis thereafter.

9.1.1 Screening Process

- **Pre-employment screening**:
    - Criminal record check (via official Curaçao authorities or equivalent international channels).
    - Verification of financial integrity (credit check, bankruptcy/insolvency records, previous regulatory sanctions or AML-related disciplinary actions).
    - Assessment of ethical standards and professional references.
    - Sanctions and PEP screening (to ensure no conflict with targeted financial sanctions).

- **Ongoing screening** for existing staff:

- Annual re-screening of criminal and financial records.
- Immediate re-screening upon promotion to higher-risk roles (e.g., customer-facing, compliance, MLRO support) or if any red-flag indicators arise.

Any adverse findings are assessed by the MLRO and senior management. Individuals with relevant criminal convictions, financial misconduct or regulatory sanctions that could compromise AML/CFT integrity will not be hired or will be subject to appropriate disciplinary action, up to and including termination.

9.2 Ongoing Employee Training Programme

The Company delivers a structured, role-tailored training programme that meets the exact requirements of Regulations V.4.

9.2.1 Frequency

- **Initial training** – Completed as part of onboarding, before the employee is allowed to perform any AML/CFT-related duties.
- **Annual refresher training** – Mandatory for all staff every calendar year.
- **Ad-hoc / targeted training** – Delivered immediately upon:

  - Introduction of new products, services, payment methods or technologies.
  - Material changes to laws, regulations or CGA guidance.
  - Identification of new ML/TF/PF trends or typologies relevant to online gaming.

9.2.2 Tailoring by Role

Training content and depth are customised according to the employee's responsibilities:

- **All staff** – Basic awareness of ML/TF/PF, red flags, no-tipping-off rules, and the Company's policies.
- **Customer-facing staff** (support, account managers, VIP team) – Detailed recognition of gambling-specific red flags, handling of CDD requests, customer interaction protocols.
- **Compliance, MLRO and risk team** – Advanced training on risk assessments (BRA/CRA), EDD, transaction monitoring, goAML reporting, PEP/sanctions handling and audit preparation.
- **Senior management / Board** – Oversight responsibilities, risk appetite, effectiveness review and reporting to the CGA.

9.2.3 Core Training Content

- Methods and typologies of money laundering, terrorist financing and proliferation financing, with specific focus on the gambling sector (placement through

chips/deposits, layering via minimal-play withdrawals, integration through winnings).
- Gambling-specific red flags (as detailed in Section 8 of this policy and Regulations II.2.3).
- Customer Due Diligence (CDD), Enhanced Due Diligence (EDD) and Simplified Due Diligence procedures, including NAf 4,000 threshold rules.
- Transaction monitoring, alert investigation and escalation processes.
- Recognition, documentation and reporting of unusual transactions (goAML process).
- Prohibition of tipping-off and confidentiality obligations.
- Sanctions screening and PEP requirements.
- Record-keeping obligations and data protection.
- The Company's internal policies, procedures and controls (including consequences of non-compliance).

Training is delivered through a combination of e-learning modules, workshops, scenario-based exercises and knowledge tests. Employees must achieve a passing score to complete each module.

9.3 Documentation and Record-Keeping

- A central training register is maintained, recording the following:
    - Date and type of training received.
    - Training content and materials provided.
    - Trainer/facilitator details.
    - Assessment results and pass/fail status.
    - Any follow-up actions required.
- Records are retained for at least five years and are available for inspection by the CGA, internal auditors or external regulators.

9.4 Effectiveness and Continuous Improvement

The MLRO conducts an annual review of the training programme's effectiveness (including feedback from staff and audit findings) and updates content as necessary. The results of this review are included in the annual AML effectiveness report to the Board.

Non-completion of required training or failure to apply learned procedures may result in disciplinary action, up to and including termination of employment.

10. Independent Audit

The Company maintains a formal independent audit function to objectively evaluate the design, implementation, and effectiveness of the entire AML/CFT/PF Compliance Programme. This audit ensures that all policies, procedures, controls, risk assessments,

training, and operational processes fully comply with the January 2025 CGA Regulations and remain adequate to mitigate identified ML/TF/PF risks.

10.1 Frequency and Scope

- An independent audit of the complete AML/CFT/PF programme is conducted at least once every calendar year.

- Additional ad-hoc audits may be triggered by:

    - Material changes to the business (new products, markets, payment methods, or technologies).
    - Significant regulatory updates or CGA guidance.
    - Identification of serious deficiencies, high volumes of unusual transaction reports, or adverse audit findings from previous reviews.
    - Request from the Board, MLRO, or Curaçao Gaming Authority (CGA).

10.2 Scope of the Audit

The audit comprehensively tests all elements of the AML/CFT/PF programme, including but not limited to:

- Business Risk Assessment (BRA) and Customer Risk Assessment (CRA) processes and documentation.
- Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Simplified Due Diligence (SDD), and the NAf 4,000 threshold procedures.
- Beneficial owner identification and verification.
- PEP and sanctions screening systems and handling protocols.
- Transaction monitoring rules, alert generation, investigation, and escalation processes.
- Recognition, documentation, and reporting of unusual transactions (including goAML filings and no-tipping-off compliance).
- Employee screening programme and ongoing training effectiveness.
- Record-keeping and retention practices (minimum five years).
- Third-party reliance and outsourcing controls.
- Risk-based approach implementation, including risk appetite, mitigation measures, and residual risk management.
- Governance arrangements (MLRO independence, Board oversight, and reporting lines).
- Overall programme effectiveness in preventing and detecting ML/TF/PF in the online gaming environment.

10.3 Audit Findings

All audit findings are documented and corrective actions must be implemented within defined timelines. The MLRO shall monitor the implementation of corrective actions and report progress to senior management.

11. Approval and Review

This Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT) and Proliferation Financing (PF) Policy, together with all associated procedures and controls, constitutes the Company's formal AML/CFT/PF Compliance Programme.

11.1 Board Approval

The policy and the entire AML/CFT/PF Compliance Programme have been reviewed and formally approved by the Board of Directors of MCG Technologies N.V. Board approval confirms that the programme is adequate, proportionate to the risks identified in the Business Risk Assessment (BRA), and fully compliant with the Curaçao Gaming Control Board (CGA) Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (January 2025), the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and all related Sanctions legislation.

11.2 Effective Date

This policy is effective immediately upon Board approval. All staff, contractors and third-party service providers must comply with its provisions from this date. Any previous versions of the AML policy are superseded.

11.3 Review and Update Process

The policy and the overall KYC/AML/CFT/PF Compliance Programme will be subject to a comprehensive annual review by the MLRO and senior management. The review assesses the continuing adequacy and effectiveness of the programme in light of:

- Changes in the Company's business activities, products, services, delivery channels or customer base.
- New or emerging ML/TF/PF risks (including technological developments).
- Amendments to Curaçao law, CGA Regulations, FATF Recommendations, or CFATF guidance.
- Findings from internal/external audits, transaction monitoring trends, or Unusual Transaction Reports.
- Any material regulatory feedback or enforcement actions.

The policy will also be reviewed and updated immediately (or as soon as practicable) upon any significant CGA regulatory update, change in the National Risk Assessment, or material change to the Company's risk profile. All revisions will be documented with a clear version history, rationale for changes, and Board re-approval.

11.4 Upload to CGA Licensee Portal

In accordance with CGA licence conditions and the January 2025 Regulations, the current version of this policy (and any future material updates) is uploaded to the CGA Licensee Portal (portal.gamingcontrolcuracao.org) within the required timeframe. The Company will maintain evidence of each successful upload.

11.5 Staff Acknowledgement and Communication

All employees, contractors and relevant third parties:

- Receive a copy of the policy.
- Complete mandatory acknowledgement confirming that they have read, understood and agree to comply with the policy.
- Attend the required AML/CFT/PF training (initial and annual) that specifically covers this policy.

The MLRO maintains a central register of all acknowledgements and training completions. Failure to acknowledge or comply with the policy may result in disciplinary action, up to and including termination of employment or contract.

11.6 Record Keeping

The approved policy, all review documentation, Board minutes of approval, staff acknowledgements, and evidence of portal uploads are retained securely for a minimum of five years (or longer if required by ongoing investigations or legal proceedings) and will be made available to the CGA or FIU upon request.

This section ensures full governance oversight, regulatory transparency and accountability as required by the Curaçao Gaming Control Board. The Board remains ultimately responsible for the effectiveness of the AML/CFT/PF Compliance Programme.

Money Laundering Reporting Officer:

Nicholas Gatt

12 June 2026

KYC_AML_CTF_and_CPF_Policy_-_Curacao_v1.0_-_MCG_Technologies_N.V..docx

Final Audit Report 2026-06-24

Created:	2026-06-24
By:	Danielle Defoe (Danielle@igatrust.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAmG-8vq5hp1W7ClKkVeB9flaslayhlCix

"KYC_AML_CTF_and_CPF_Policy_-_Curacao_v1.0_-_MCG_Technologies_N.V..docx" History

Document digitally presigned by DocuSign\, Inc. (enterprisesupport@docusign.com)
2026-06-23 - 9:19:22 AM GMT- IP address: 190.104.107.51

Document created by Danielle Defoe (Danielle@igatrust.com)
2026-06-24 - 2:22:48 PM GMT- IP address: 190.104.107.51

Document emailed to Claire Godschalk (Claire@igatrust.com) for signature
2026-06-24 - 2:26:26 PM GMT

Email viewed by Claire Godschalk (Claire@igatrust.com)
2026-06-24 - 3:52:36 PM GMT- IP address: 104.47.18.126

Document e-signed by Claire Godschalk (Claire@igatrust.com)
Signature Date: 2026-06-24 - 3:53:43 PM GMT - Time Source: server- IP address: 151.43.97.162 - Signature Appearance Selected: MOBILE_IMAGE

Agreement completed.
2026-06-24 - 3:53:43 PM GMT