

OPERATIONAL MANUAL

MCG Technologies N.V.

Zuikertuintjeweg Z/N, Curaçao

CGA Licence Number: OGL/2024/1698/0936

Company Reg. Number: 166630

Document Reference: MCG-OM-2026-V1.0

Version: 1.0

Effective Date: June 2026

Review Date: June 2027

Gaming Website(s): www.luckysplash.io/www.21.com

ADR Provider: CADRE B.V. (www.cadre.online)

This Operational Manual is issued pursuant to Article 5.9 of the National Ordinance on Games of Chance (Landsverordening op de kansspelen — "LOK"), PB 2024, no. 157, and in compliance with the regulatory framework established by the Curaçao Gaming Authority (CGA).

CONFIDENTIAL | For regulatory and internal use only.

Version Control

Ver.	Date	Author	Changes
1.0	June 2026	Board of Directors	Initial version prepared and approved

Board Approval of Policy

Date of Approval: 15th June, 2026

Table of Contents

Version Control

1. Introduction & Corporate Overview
2. Regulatory Framework & Licence Compliance
3. Corporate Governance & Management Structure
4. Platform & Technical Infrastructure
5. Gaming Products & Services
6. Player Registration & Account Management
7. Know Your Customer (KYC) & Identity Verification
8. AML/CTF/PF Compliance Programme
9. Responsible Gaming Programme
10. Complaints Handling & Alternative Dispute Resolution
11. Payment Processing & Financial Controls
12. Information Security
13. Data Protection & Privacy
14. Marketing & Advertising Standards
15. Third-Party & Vendor Management
16. Staff Recruitment, Screening & Training
17. Regulatory Reporting & Record Keeping
18. Business Continuity & Disaster Recovery
19. Anti-Fraud & Game Integrity
20. Policy Review & Document Control

Appendix A: Regulatory Reference List

Appendix B: Key Contacts

Appendix C: Glossary of Key Terms

Appendix D: Restricted Jurisdictions Policy

1. Introduction & Corporate Overview

1.1 Purpose of this Manual

This Operational Manual ("the Manual") has been prepared by MCG Technologies N.V. ("the Company", "MCG", "we", "us") in accordance with Article 5.9 of the National Ordinance on Games of Chance (Landsverordening op de kansspelen — "LOK"), PB 2024, no. 157, effective 24 December 2024.

The Manual documents the procedures, controls, policies, and governance arrangements in place across all areas of the Company's online gaming operations. It constitutes the primary reference document for staff, management, third-party partners, and the Curaçao Gaming Authority (CGA) concerning how the Company manages its licensed activities.

1.2 Company Profile

Item	Details
Legal Name	MCG Technologies N.V.
Registered Address	Zuikertuintjeweg Z/N
Registration Number	166630
CGA Licence Number	OGI/2024/630/1003
Gaming Website(s)	www.21.com / www.luckysplash.io
Platform Provider	Pragmatic Gaming Solutions
ADR Provider	CADRE B.V. (www.cadre.online)

1.3 Business Overview

MCG Technologies N.V. is an online gaming operator licensed by the Curaçao Gaming Authority (CGA) to offer remote gaming services, including Live Casino, Casino, and Sportsbook products, through its gaming websites. The Company operates on a platform provided and maintained by Pragmatic Gaming Solutions under a formal outsourcing arrangement.

The Company integrates games directly from leading providers (Pragmatic Play, Evolution, IMK365, Ruby) and accesses an extended games library through aggregator partnerships with Hub88 and Alea.

1.4 Scope of this Manual

This Manual applies to:

- All directors, officers, internal employees, and contractors of MCG Technologies N.V.;
- All gaming products and services offered on the Company's licensed websites;
- All third-party service providers, including platform operators, payment processors, gaming suppliers, aggregators, and affiliates;
- All delivery channels, including web browser, mobile web, and any future mobile applications.

2. Regulatory Framework & Licence Compliance

2.1 Applicable Legislation & Regulations

The Company's operations are governed by the following primary regulatory instruments:

1. National Ordinance on Games of Chance (LOK) — PB 2024, no. 157 (effective 24 December 2024) — the primary enabling legislation for online gaming in Curaçao.
2. CGA Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction (Version 10 January 2025).
3. National Ordinance on Identification when Rendering Services (LID).
4. National Ordinance on the Reporting of Unusual Transactions (LMOT).
5. CGA Responsible Gaming Policy (Version 1.0, 17 April 2025).
6. CGA Player Complaints Policy Guidelines (Version 1.1, 18 June 2025).
7. CGA ADR Role and Certification Guidelines (Version 1.0, 8 September 2025).
8. Kingdom of the Netherlands Sanctions Act and all applicable UN/EU sanctions regulations.
9. FATF Recommendations (as applicable to online gaming operators).
10. All CGA Licence Conditions attached to Licence No. OGL/2024/630/1003.

2.2 CGA Licence

Licence Number: OGL/2024/630/1003

Licence Holder: MCG Technologies N.V.

Regulator: Curaçao Gaming Authority (CGA)

Authorised Activities: Remote online gaming — Live Casino, Casino (RNG), Sports Betting

Authorised Domains: www.luckysplash..io/www.21.com

The Company's CGA licence is displayed prominently on its gaming websites in the footer, together with the CGA digital seal. The licence number and regulatory information are accessible to players at all times.

2.3 Regulatory Compliance Obligations

- Upload of all required policies and procedures to the CGA Licensee Portal (portal.gamingcontrolcuracao.org) within mandated timeframes;
- Submission of periodic reports to the CGA as required (financial reports, complaints data, AML/CTF reports, responsible gaming reports);
- Immediate notification to the CGA of material changes to business operations, corporate structure, or key personnel;
- Co-operation with all CGA inspections, audits, and requests for information;
- Maintenance of records available for CGA inspection for a minimum of five (5) years, unless a longer period is required by law;
- Annual policy review cycle aligned with the CGA regulatory calendar.

2.4 Designated Regulatory Contact

The Company designates a Compliance Officer-Nicholas Gatt as the primary point of contact for the CGA together with the Corporate Service Provider who will be IGA Trust going forward. All regulatory

correspondence is routed through IGA Trust (however, currently the CSP is G-Force Corporate) the Compliance Officer together with IGA Trust will be responsible for:

- Monitoring and implementing regulatory changes;
- Maintaining the CGA Portal account and submission schedule;
- Co-ordinating responses to CGA enquiries;
- Reporting material incidents or breaches to the CGA without undue delay.

2.5 Material Changes

Any material change to the Company's operations, structure, or key personnel must be notified to the CGA prior to implementation (or as soon as practicable in emergencies). Material changes include:

- Change in ultimate beneficial ownership;
- Addition or removal of directors;
- Addition of new gaming verticals or significant product changes;
- Change of platform provider;
- Addition of new website domains;
- Change of payment methods offered to players.

3. Corporate Governance & Management Structure

3.1 Board of Directors

The Company is governed by its Board of Directors, which bears ultimate responsibility for:

- Strategic direction and business oversight;
- Approval of key policies (AML/CTF, Responsible Gaming, Complaints Handling, this Operational Manual);
- Risk appetite definition and oversight;
- Ensuring adequate resources for compliance and regulatory obligations;
- Receiving and reviewing periodic reports from the Compliance function, MLRO, and Responsible Gaming Officer.

Name	Role
IGA Trust	Director

3.2 Key Management Functions

Role	Responsibilities
Compliance Officer	Regulatory liaison; policy management; CGA portal; licence conditions oversight
Money Laundering Reporting Officer (MLRO)	AML/CTF/PF programme oversight; UTR reporting; PEP/sanctions escalation; Board reporting
Responsible Gaming Officer	RG programme management; player intervention oversight; RG reporting to CGA
Complaints Officer	Complaints intake, investigation and resolution; ADR coordination
Data Protection Officer (DPO)	GDPR/data protection compliance; breach notification
Head of Customer Support	Day-to-day player service; first-line KYC support; RG escalation
Head of Payments	Payment processing oversight; fraud monitoring; chargebacks

3.3 Governance Principles

- Segregation of duties: Compliance, MLRO, and Responsible Gaming functions operate independently from commercial operations.
- Escalation paths: Clear escalation routes exist for all compliance, AML, responsible gaming, and complaints matters.
- Board oversight: The Board receives quarterly reports from key compliance functions and approves all material policy changes.
- Documentation: All key decisions, approvals, and governance actions are documented and retained.
- Proportionality: Governance structures are proportionate to the size and complexity of the business and the risks identified.

3.4 Policy Approval & Review

All policies within the Company's compliance framework are:

- Reviewed and approved by the Board of Directors;

- Subject to annual review (at minimum);
- Reviewed immediately upon material regulatory changes or significant business events;
- Version-controlled and stored securely;
- Uploaded to the CGA Licensee Portal where required.

4. Platform & Technical Infrastructure

4.1 Platform Outsourcing Arrangement

The Company's gaming platform is operated by Pragmatic Gaming Solutions ("the Platform Provider") under a formal outsourcing agreement. The Platform Provider is responsible for:

- Hosting and maintaining the technical gaming environment;
- Integration with gaming content providers and payment processors;
- Front-end website operations for www.lucksplash.io/www.21.com;
- System availability, uptime, and performance management;
- Technical compliance with CGA technical standards;
- Security of the gaming infrastructure.

Note on Regulatory Responsibility: Notwithstanding the outsourcing of the platform to Pragmatic Gaming Solutions, MCG Technologies N.V. retains full regulatory responsibility for all aspects of its licensed operations. The outsourcing arrangement does not relieve the Company of its obligations under the LOK or CGA licence conditions.

4.2 Outsourcing Governance

The Company ensures appropriate oversight of the Platform Provider through:

- A formal written outsourcing/service agreement clearly defining roles, responsibilities, SLAs, and compliance obligations;
- Regular performance reviews and SLA monitoring;
- Right-to-audit clauses enabling the Company and the CGA to inspect the Platform Provider's operations;
- Data processing agreements compliant with applicable data protection legislation;
- Incident notification requirements (Platform Provider must notify the Company within 24 hours of any material incident);
- Confirmation that the Platform Provider maintains ISO/IEC 27001-aligned information security practices (as documented in Pragmatic Solutions' Information Security Policy V2.6, October 2025).

4.3 Information Security Framework

Pragmatic Gaming Solutions maintains a comprehensive information security policy (V2.6, October 2025) aligned with ISO/IEC 27001, covering:

- Asset management and data classification (DCL1 Public / DCL2 Sensitive);
- Personnel security including pre-employment screening and role-based training;
- Physical and environmental controls;
- Access control (unique IDs, 60-day password rotation, 12-character minimum passwords, MFA);
- Secure development, change management, and code review processes;
- Operational controls (backups, encryption, logging, patch management);
- Incident response (identification, classification, containment, eradication, recovery);
- Business continuity and disaster recovery.

4.4 Authorised Domains

The Company operates gaming services exclusively through the following CGA-authorised domains:

- www.luckysplash.io
- www.21.com

Any additional domains require prior CGA approval and amendment of the licence before activation.

4.5 Technical Standards & RNG Certification

All Random Number Generators (RNGs) used in casino games must be independently certified by an approved testing laboratory. Certificates of conformity are maintained and made available to the CGA upon request.

4.6 Geolocation & Player Origination

The Platform Provider implements geolocation technology to:

- Determine a player's country of origin at registration and login;
- Block access from jurisdictions where the Company's services are restricted or prohibited;
- Support AML/CTF risk assessment by flagging high-risk geographic origins.

The Company maintains and regularly updates its list of restricted jurisdictions. Players from restricted jurisdictions are blocked from registration and play.

5. Gaming Products & Services

5.1 Authorised Gaming Verticals

Vertical	Description
Live Casino	Real-time casino games hosted by professional dealers, including Live Roulette, Live Blackjack, Live Baccarat, Live Game Shows, and other live-hosted variants. Streamed in real time to players.
Casino (RNG)	Electronic casino games powered by certified Random Number Generators (RNG), including video slots, table games, instant win games, and jackpot titles.
Sportsbook	Fixed-odds and in-play betting on domestic and international sporting events, including football, basketball, tennis, and other sports markets.

5.2 Gaming Content Providers

5.2.1 Direct Integrations

Provider	Product Category
Pragmatic Play	Slots, Live Casino, Bingo, Virtual Sports
Evolution	Live Casino, Game Shows
IMK365	Slots, Table Games
Ruby	Slots

5.2.2 Aggregator Partners

Aggregator	Role
Hub88	Multi-provider aggregation platform providing access to a broad portfolio of casino and live dealer content
Alea	Aggregation and distribution of casino game content with enhanced back-office reporting

5.3 Third-Party Provider Due Diligence

All gaming providers and aggregators are subject to due diligence prior to onboarding and on an ongoing basis:

- Verification of the provider's regulatory licences and certifications;
- Assessment of the provider's compliance posture (AML, data protection, information security);
- Review of terms of service and revenue sharing or integration agreements;
- Annual review of the provider relationship.

5.4 Game Fairness & Integrity

- All RNG-based games use independently EU certified RNGs.
- Return-to-Player (RTP) information for all casino games is made available to players.
- The Company does not offer or permit cheating tools, bots, or any system designed to gain an unfair advantage.
- Live casino games are streamed from licensed studios with professional croupiers.

- Sports betting odds are set and managed in compliance with applicable rules and the Company's sportsbook terms.

6. Player Registration & Account Management

6.1 Player Eligibility

Players must meet the following minimum eligibility criteria before an account may be created:

- Minimum age of 18 years (or the higher legal minimum gambling age in the player's jurisdiction of residence);
- Not resident in a jurisdiction from which the Company's services are restricted or prohibited;
- Not subject to self-exclusion on any of the Company's brands;
- Not a current employee, director, or immediate family member of an employee or director of the Company or any of its key suppliers.

6.2 Registration Process

6.2.1 Registration Requirements

At account creation, players must provide:

- Full legal name;
- Permanent residential address;
- Date of birth;
- Email address;
- Mobile telephone number;
- Username and secure password (minimum 8 characters including uppercase, lowercase, and numeric characters);
- Confirmation of age (mandatory checkbox confirming the player is 18 or over);
- Confirmation of acceptance of the Terms & Conditions and Privacy Policy;
- Confirmation of not being self-excluded.

6.2.2 Age Verification at Registration

The Company applies a multi-step age verification process:

11. Self-attestation: Players confirm their date of birth and tick a mandatory age declaration checkbox at registration.
12. System risk flagging: Suspicious or obviously invalid dates of birth, email addresses, or payment details previously associated with underage access trigger automatic review.
13. Document verification: No player may make a first withdrawal or exceed the AML verification threshold without submitting government-issued photo ID (passport, national ID card, or driver's licence). Screenshots or cropped documents are not accepted.

6.2.3 Discovery of Minors

If the Company becomes aware that a minor has gained access:

- The account is closed immediately;
- All deposits are refunded;
- All winnings are forfeited in accordance with legal requirements;
- The case is escalated to the Responsible Gaming Officer and documented;
- Records are retained for audit and retained for a minimum of five years.

6.3 Account Management

6.3.1 Account Security

- Each player has a unique account with a unique username;
- Players are advised to use strong passwords and not to share account credentials;
- Multi-factor authentication (MFA) options are available;
- Unattended or inactive sessions are automatically logged out after a defined inactivity period;
- Players can access their full account history at all times via the account dashboard.

6.3.2 Account Restrictions

- A player may hold only one account per brand;
- Duplicate accounts are detected and merged or closed;
- The Company may suspend or close an account at any time for breach of terms and conditions, fraud, AML concerns, or regulatory requirements.

6.3.3 Account Closure

Players may request account closure at any time. Upon closure:

- Available balances (after satisfaction of applicable bonus wagering requirements) are returned to the player via their last used payment method;
- The Company retains records of the account and all associated data for the required minimum retention period;
- If closure is requested in connection with responsible gaming concerns, the Responsible Gaming Officer is notified.

6.3.4 Dormant Accounts

Accounts with no login or activity for 12 consecutive months are classified as dormant. The Company:

- Notifies the player prior to the account being deemed dormant;
- Continues to safeguard any player funds in the dormant account;
- Applies dormant account fees only where explicitly permitted under the Terms & Conditions and applicable law;
- Maintains dormant account records for the full regulatory retention period.

7. Know Your Customer (KYC) & Identity Verification

7.1 Overview

The Company's KYC programme is designed to verify the identity of all players in accordance with the CGA AML/CTF Regulations (January 2025) and the National Ordinance on Identification when Rendering Services (LID). KYC obligations apply at account opening and on an ongoing basis.

7.2 When KYC/CDD is Required

Customer Due Diligence (CDD) is required:

- At account opening (minimum identification information);
- When cumulative financial transactions (deposits/withdrawals/transfers) reach or exceed NAF 4,000 in a single day (linked transactions within the same session are aggregated);
- For occasional transactions of NAF 4,000 or more;
- When there is suspicion of money laundering, terrorist financing, or proliferation financing;
- When there are doubts about the accuracy of previously obtained customer data;
- Before processing any withdrawal that would trigger the CDD threshold.

7.3 Minimum Identification Information

At account opening, the following minimum information is collected from all players regardless of risk level:

- Full legal name;
- Permanent residential address;
- Date of birth.

7.4 Identity Verification Documents

7.4.1 Primary Identity Document (Mandatory)

A government-issued photo ID is required for full verification. Accepted documents:

- Passport;
- National identity card;
- Driver's licence.

Documents must be: clear (not blurred or obscured), valid (not expired), and match the registration data. Screenshots or cropped documents are not accepted.

7.4.2 Proof of Address

Proof of address is required for full KYC clearance. Accepted documents:

- Utility bill (gas, electricity, water, telephone) issued within the last 6 months;
- Bank statement issued within the last 6 months;
- Fixed-line phone bills are accepted.

7.4.3 Additional Verification (High-Risk)

For high-risk players, additional information and verification may be required:

- Place of birth, nationality, identity number, occupation;
- Source of wealth and source of funds documentation;

- Biometric / selfie match; Video call verification;
- Geolocation / IP / device fingerprinting;
- Third-party database checks.

7.5 Termination for Non-Compliance

If a player fails to complete required KYC/CDD within 30 days of reaching the NAF 4,000 threshold:

- The account is blocked;
- The business relationship is terminated;
- The transaction is assessed for potential reporting to the FIU via goAML;
- All attempts to obtain CDD documentation are documented and retained for at least five years.

Where there is no suspicion of money laundering, remaining player funds are returned via the original deposit channel.

7.6 Record Keeping

All KYC records (documents submitted, verification outcomes, communications, and decisions) are stored securely for a minimum of five years from the end of the business relationship. Records are available for inspection by the CGA upon request.

8. Anti-Money Laundering, Countering the Financing of Terrorism & Proliferation Financing (AML/CTF/PF) Compliance Programme

8.1 Policy Statement

MCG Technologies N.V. maintains a zero-tolerance approach towards money laundering, terrorist financing, and proliferation financing. The Company's AML/CTF/PF Compliance Programme is designed to prevent the Company from being used for illicit financial activities and to ensure full compliance with all applicable Curaçao laws, CGA regulations, and FATF recommendations. All employees, contractors, and third-party service providers are required to comply with this programme.

8.2 Money Laundering Reporting Officer (MLRO)

MLRO Responsibilities:

- Oversight of the entire AML/CTF/PF Compliance Programme
- Maintenance and review of the Business Risk Assessment (BRA)
- Review and approval of high-risk customer onboarding
- Receipt and assessment of internal Suspicious Activity Reports
- Submission of Unusual Transaction Reports (UTR) to the FIU via goAML
- Annual AML effectiveness report to the Board

The MLRO operates independently from operational functions and has unrestricted access to all relevant data, the authority to block transactions, and the authority to submit reports to the FIU without prior management approval.

8.3 Business Risk Assessment (BRA)

The Company conducts a comprehensive, documented Business Risk Assessment (BRA) to identify, analyse, and evaluate all ML/TF/PF risks. The BRA covers four core risk categories:

14. Customer Risk: PEPs, high spenders, irregular income, third-party play, multiple accounts.
15. Geographical Risk: Player nationality, residence, high-risk jurisdictions (FATF lists, EU strategic deficiencies, OFAC sanctions, Transparency International CPI).
16. Product, Service & Transaction Risk: Anonymous payment methods, minimal-play withdrawals, peer-to-peer transfers, structuring.
17. Distribution Channel Risk: Non-face-to-face onboarding, involvement of third parties.

The BRA is:

- Approved by the Board of Directors;
- Reviewed at least annually;
- Immediately reviewed upon material changes (new products, markets, payment methods, regulatory updates);
- Available to the CGA upon request;
- The foundation of the Customer Acceptance Policy (CAP).

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

Each player is subject to a Customer Risk Assessment (CRA) that assigns a risk rating:

Rating	Criteria	Review Time
Low	Stable profile, transparent source of funds, low-value regular activity, low-risk jurisdiction	5 business days
Medium	Moderate deviations, higher-risk payment methods mitigable by controls	3 business days
High	PEPs, disproportionate spending, anonymous/high-risk payments, high-risk jurisdictions, multiple red flags	24 hours

High-risk customer onboarding requires MLRO/Compliance Officer review and senior management approval. All acceptance and rejection decisions are documented.

8.5 Sanctions & PEP Screening

8.5.1 Sanctions Screening

All players (and beneficial owners) are screened against:

- UN Security Council Consolidated List;
- EU Sanctions Map;
- Curaçao / Kingdom of the Netherlands sanctions lists;
- OFAC (as applicable for risk mitigation).

Screening lists are updated at least monthly (or immediately upon new sanctions designations). Automated screening is supplemented by manual verification of all hits. Where a sanctioned person is identified: all funds are frozen immediately, the MLRO is notified, and a report is submitted to the FIU.

8.5.2 PEP Screening

PEP screening covers domestic, foreign, and international organisation PEPs, plus their family members and close associates. Screening occurs at onboarding and on an ongoing automated and periodic manual basis.

PEPs require: senior management approval; source of wealth/funds documentation; enhanced ongoing monitoring.

8.6 Transaction Monitoring

The Company operates a risk-based transaction monitoring programme combining automated rules-based monitoring with manual MLRO/analyst review:

Alert Type	Review Timeframe	Oversight
High-risk	Within 24 hours	Anti Fraud Team and raised to MLRO
Medium-risk	Within 3 business days	Anti Fraud Team
Low-risk	Within 5 business days	Anti Fraud team

8.6.1 Red Flags & Indicators

The Company monitors the following red flags (among others):

- Deposit followed by immediate withdrawal with minimal or no play ("in-and-out" / "parking");
- 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 fund transfers between accounts;

- Use of anonymous or high-risk payment methods (crypto, prepaid cards, e-wallets);
- Player from or funds sourced from high-risk jurisdictions;
- PEPs or close associates;
- Third-party deposits or withdrawals;
- Identity fraud indicators;
- Any transaction (single or linked series) of NAf 5,000 or more.

8.7 Unusual Transaction Reporting

Where a transaction cannot be satisfactorily explained and cannot be excluded from suspicion of ML/TF/PF:

- An Unusual Transaction Report (UTR) is filed to the FIU Curaçao via the goAML portal without delay;
- No tipping-off: Employees are strictly prohibited from disclosing to any player or third party that an investigation is underway or that a report has been filed. Breach of this prohibition constitutes a serious compliance violation.

8.8 AML/CTF Record Keeping

All AML/CTF records (CDD data, transaction records, monitoring logs, UTR documentation) are retained for a minimum of five years and are readily available for CGA and FIU inspection.

9. Responsible Gaming Programme

9.1 Policy Statement

MCG Technologies N.V. is committed to providing a safe and responsible gaming environment for all players. The Company recognises that gambling can pose risks to a minority of players and maintains a comprehensive Responsible Gaming (RG) programme to prevent problem gambling and protect vulnerable individuals, including minors. We also have the policy on the footer of our website which is accessible from every page.

9.2 Responsible Gaming Officer

The internal Responsible Gaming Officer (RGO) has oversight responsibility for the entire RG programme, including:

- Monitoring the effectiveness of RG tools and interventions;
- Reviewing player escalations and authorising enhanced interventions;
- Submitting an RG effectiveness report to management at least annually;
- Reporting material policy changes to the CGA;
- Training oversight.

9.3 Mandatory Responsible Gaming Features

The Company implements the following nine core RG elements as mandated by the CGA:

9.3.1 Age Verification

As detailed in Chapters 6 and 7 of this Manual, no player under the age of 18 may participate in any gaming activity. Multi-stage age verification is applied at registration and at the KYC verification stage. Discovery of minors results in immediate account closure, deposit refund, and forfeiture of winnings.

9.3.2 Accessible Responsible Gaming Information

- A dedicated Responsible Gaming Section is available on the Company's gaming websites at all times, containing: information on responsible gambling practices; direct access to RG tools (self-exclusion, cooling-off, deposit limits); contact details for RG support.
- A clear and visible link to the RG Section is displayed on the website homepage.
- Terms & Conditions reference the RG Section and inform players of available tools.
- The website footer displays: a warning that underage gambling is prohibited; the Company's name, address, and CGA licence number; a statement of CGA regulatory oversight; the CGA digital seal; links to GambleAware.
- Content is available in English and the language(s) of target markets.

9.3.3 Player Self-Assessment Tools

- Players can access the Gamblers Anonymous 20-Question Quiz through the RG Section.
- Players with 0 "Yes" answers: low risk. 1 "Yes" answer: moderate risk. 2+ "Yes" answers: high risk — further evaluation and intervention are recommended.
- Players who self-identify risky behaviour are advised to use deposit limits, cooling-off, or self-exclusion.
- Full account transaction history is accessible in-account; extended histories are available upon request within 10 working days.

9.3.4 Gambling Behaviour Tracking

The Company's systems and staff monitor the following indicators of problematic gambling:

- Sudden increases in deposit or wagering activity;
- Repeated failed transactions due to insufficient funds;
- Frequent reversal of withdrawal requests;
- Extended, unexplained gaming sessions;
- Excessive or agitated contact with customer support;
- Repeated changes to RG tools;
- Attempts to circumvent controls by creating multiple accounts.

A risk-based profiling system flags players exhibiting these behaviours. Interventions are proportionate and documented, including: promotion of RG tools, imposition of temporary limits, account suspension, or permanent exclusion. All interventions are logged in the Player Management System and retained for a minimum of five years.

9.3.5 Cooling-Off & Self-Exclusion

Feature	Cooling-Off	Self-Exclusion
Wagering	Prohibited (all or by vertical)	Prohibited (all verticals)
Deposits	Not permitted	Not permitted
Withdrawals	Permitted	Subject to applicable law
Login	Permitted	Not permitted
Scope	Current brand, or all operator brands	All brands/domains under licence
Duration	Min 24 hours; options: 24h, 7 days, 1 month, 3 months	Min 1 year; options: 1, 3, 5, 10 years, or lifetime
Marketing	Mandatory opt-out	All marketing blocked
Reactivation	Automatic (no action required)	Player-initiated, after expiry

Both tools take immediate effect upon player confirmation. Where a request is submitted via customer support, the restriction is activated within 24 hours.

⚠ Important: Responsible Gaming measures will never be misused to delay withdrawals. Any withdrawal request from a player who is cooling off or self-excluded (to the extent permitted) must be processed in accordance with normal withdrawal timelines.

9.3.6 Deposit Limits

- Players may set daily, weekly, or monthly deposit limits at any time via their account settings.
- Once a limit is reached, no further deposits are accepted until the period resets.
- Requests to reduce (make more restrictive) a deposit limit take effect immediately.
- Requests to increase (make less restrictive) a deposit limit are subject to a minimum 24-hour cooling-off period before implementation.
- Any ante-post bets placed before a deposit limit is set are not affected, but no new bets may be placed while an unresolved ante-post bet remains active post-restriction.

9.3.7 Responsible Advertising & Marketing

The Company prohibits the following in all marketing and advertising:

- Targeting of vulnerable groups or persons who appear to be under 18;
- Portraying gambling as an investment or income-generating activity;
- Implying that chance-based games can be influenced by skill;
- Emotional manipulation (gambling as a solution to personal or financial problems);
- Use of minors in advertising;
- Explicit sexual or pornographic content;
- Association of gambling with alcohol, drugs, or harmful behaviours.

9.3.8 Staff Training in Responsible Gaming

All customer-facing and RG staff receive:

- Initial RG training during onboarding;
- Annual refresher training;
- Ad-hoc training upon introduction of new RG tools, policy changes, or regulatory updates.

Training covers: identification of gambling-related distress; handling of sensitive player interactions; escalation procedures; use of RG tools; available support services. Training records are retained for a minimum of five years.

9.3.9 Operator-Initiated Exclusion

The Company may impose mandatory exclusion if:

- A player exhibits signs of problematic gambling behaviour (based on documented indicators);
- There is suspicion or evidence of criminal activity.

Exclusions are never based on a player's winnings. All operator-initiated exclusions require documented indicators and approval by the RGO or Compliance function.

9.4 Prohibition on Credit

The Company does not extend credit to players under any circumstances. All gaming activity must be funded from pre-deposited player funds.

10. Complaints Handling & Alternative Dispute Resolution

10.1 Overview

This chapter establishes the Company's complaints handling procedure in accordance with Article 5.3 of the LOK and the CGA Player Complaints Policy Guidelines v1.1 (18 June 2025). All players are entitled to a free and fair complaints process, including access to Alternative Dispute Resolution (ADR) provided by the Company's CGA-certified ADR provider.

10.2 Definition of a Complaint

A complaint is any written expression of dissatisfaction with the Company's services, products, conduct, or decisions submitted by a registered player expecting a resolution. This includes: delayed withdrawals, disputed game outcomes, account issues, bonus disputes, and responsible gaming concerns. Routine customer service queries are handled under normal support procedures and are not treated as formal complaints.

10.3 Roles & Responsibilities

- Customer Support Team: First point of contact; receipt of complaints; routing to Complaints Officer.
- Complaints Officer / Compliance Department: Formal acknowledgement within 2 business days; independent investigation; written response within 15 business days (extendable to 30 days for complex cases); maintenance of complaints register; records retained for at least 7 years.
- Management: Ensures independence and adequate resources for the complaints process; reviews complaint trends quarterly.
- Third-Party Providers: Must report complaints affecting the Company within 48 hours and cooperate fully with investigations.

10.4 How to Submit a Complaint

Players may submit complaints via:

- Email: [Insert complaints email address]
- Live Chat: Available 24/7 on the Company's gaming websites
- Downloadable Complaint Form: Available on the website in English and relevant languages

A complaint must be submitted within 6 months of the date of the incident or bet settlement. Each complaint is assigned a unique reference number, categorised, and recorded in the central complaints register.

10.5 Complaints Handling Process

10.5.1 Responsible Gaming Complaints (Priority Cases)

18. Acknowledgement within 2 business days (in writing, with process explanation and estimated timeline).
19. Target resolution within 5 business days.
20. Maximum extension: 2 additional weeks with written justification and notification to the player.
21. All RG complaints are escalated to the Responsible Gaming Officer.

10.5.2 Other Complaints

22. Acknowledgement within 1 week (in writing, with process explanation and estimated timeline).
23. Target resolution within 4 weeks.

24. One-time extension of up to 4 additional weeks (with prior written notice to the player) for complex cases.

10.5.3 Final Response

The final response includes:

- A reasoned assessment of the outcome with supporting evidence;
- If the complaint is rejected: detailed reasons;
- Information on the player's right to escalate to the Company's ADR provider.

10.6 Alternative Dispute Resolution (ADR)

ADR Provider: CADRE B.V.

Website: www.cadre.online

CGA Certification: Yes

Cost to Player: Free (all costs borne by the operator)

ADR Decision: Binding on the operator

Players may initiate ADR with CADRE B.V. if:

- They submitted a valid complaint via the Company's official form;
- The Company issued a final response, or failed to resolve within the stated timeframes;
- They remain dissatisfied with the outcome.

The Company maintains a formal agreement with CADRE B.V., bears all ADR costs, and complies with all ADR decisions. All ADR cases are tracked and documented.

10.7 CGA Reporting

The Company reports complaints data to the CGA via the CGA Online Portal twice yearly, including:

- Total complaints received;
- Complaints settled (upheld and rejected);
- Pending / unresolved complaints;
- Complaints by category;
- Complaints referred to ADR;
- Complaints involving legal action by players.

11. Payment Processing & Financial Controls

11.1 General Principles

- Player funds are maintained separately from Company operational funds;
- No credit is extended to players;
- All payment methods offered to players are subject to AML/CTF risk assessment;
- The Company is responsible for all payment processing activity, including that conducted via the Platform Provider.

11.2 Accepted Payment Methods

The Company offers a range of deposit and withdrawal options, which may include:

- Major credit and debit cards (Visa, Mastercard);
- E-wallets (subject to AML risk assessment);
- Bank transfers;
- Cryptocurrencies (where permitted and subject to enhanced due diligence and blockchain analytics).

11.3 Player Fund Segregation

Player funds are held in a dedicated account or accounts, separate from the Company's operational funds. The Company maintains records of all player fund balances and transactions.

11.4 Deposits

- Deposits are processed in real time or as quickly as technically possible;
- Third-party deposits (i.e., deposits from an account not belonging to the verified player) are not accepted;
- Deposits from sanctioned persons or high-risk sources are blocked;
- The AML/CTF threshold of NAf 4,000 triggers mandatory KYC verification before further transactions are processed.

11.5 Withdrawals

- Withdrawals are processed promptly upon completion of applicable identity verification;
- Withdrawals must be made to the same method used for the original deposit (same-source principle) where technically possible;
- Withdrawal requests are reviewed for AML red flags before processing;
- Responsible Gaming measures (cooling-off, self-exclusion) do not delay legitimate withdrawals to the extent permitted by applicable law;
- Withdrawal processing times are disclosed clearly in the Terms & Conditions.

11.6 Chargebacks & Fraud

- The Company maintains a chargeback management process;
- Accounts subject to confirmed fraud are suspended pending investigation;
- Fraudulent activity is reported to the MLRO for assessment and potential UTR filing;
- The Company reserves the right to offset chargeback losses against pending withdrawals where fraud is confirmed.

11.7 Financial Reporting

The Company submits financial reports to the CGA as required by licence conditions, including:

- Gross Gaming Revenue (GGR) reports;
- Player fund reports;
- Transaction volumes and values as requested.

12. Information Security

12.1 Framework

The Company's information security requirements are primarily fulfilled through its outsourcing arrangement with Pragmatic Gaming Solutions, which maintains an Information Security Policy aligned with ISO/IEC 27001 (Version 2.6, October 2025). The Company requires the Platform Provider to maintain this standard at all times.

12.2 Key Security Controls

12.2.1 Access Control

- Unique user IDs for all staff and system accounts;
- Passwords must be changed every 60 days, be at least 12 characters, and include upper/lowercase letters and at least two numeric or symbol characters;
- Credentials must not be shared or written down;
- Unattended sessions must be locked or terminated;
- Least privilege principle applied to all system access;
- Separate production vs. test/staging credentials;
- Prompt deactivation of access for leavers.

12.2.2 Data Classification

- DCL1 — Public: Information approved for public disclosure.
- DCL2 — Sensitive: Confidential player data, financial data, compliance records; subject to encryption and restricted access.

12.2.3 Encryption

- Sensitive data is encrypted on disk and on backup media;
- Encryption key management prevents disclosure, supports secure distribution, centralised management, audit logging, and key rotation;
- No single administrator may access actual encryption keys unilaterally.

12.2.4 Operational Controls

- Documented operating procedures for all critical processes;
- Segregation of duties for sensitive functions;
- Production backups with off-site storage;
- Restore testing conducted periodically;
- Protected system logging with periodic log reviews;
- Clock synchronisation across all systems.

12.3 Incident Management

All staff are required to report any suspected security weakness or incident. The incident response process follows: identification → severity classification → containment → eradication → recovery → root-cause analysis → lessons learned. Management, legal counsel, and the DPO determine breach notification duties, including notification to the CGA and affected players where required by law.

12.4 Penetration Testing & Vulnerability Management

- Security compliance checks are conducted at least annually;
- Production environments are redundant, hardened, patched, and free from known unmitigated vulnerabilities;
- Vulnerability assessments and penetration tests are conducted at least annually or upon material changes to the platform.

13. Data Protection & Privacy

13.1 Regulatory Basis

The Company processes personal data of players and employees in compliance with applicable data protection laws, including the Kingdom of the Netherlands' data protection legislation and, to the extent applicable, the EU General Data Protection Regulation (GDPR).

13.2 Data Protection Principles

- Lawfulness, fairness, and transparency: Data is processed only on a lawful basis and players are informed of how their data is used.
- Purpose limitation: Data is collected for specified, explicit, and legitimate purposes and not further processed in an incompatible manner.
- Data minimisation: Only data that is necessary for the stated purpose is collected.
- Accuracy: Reasonable steps are taken to ensure data is accurate and kept up to date.
- Storage limitation: Data is not retained longer than necessary.
- Integrity and confidentiality: Appropriate security measures are applied.
- Accountability: The Company is responsible for demonstrating compliance.

13.3 Data Protection Officer (DPO)

The Company appoints a Data Protection Officer responsible for:

- Monitoring compliance with data protection obligations;
- Advising on data protection impact assessments;
- Acting as contact point for data subjects and regulatory authorities;
- Managing data breach response and notification.

13.4 Player Data

Players are informed of their data rights via the Company's Privacy Policy. Players' data rights include:

- Right of access to their personal data;
- Right to rectification of inaccurate data;
- Right to erasure (subject to legal retention obligations);
- Right to data portability;
- Right to object to processing.

13.5 Data Retention

Data Category	Minimum Retention Period
KYC / Identity verification records	5 years from end of business relationship
AML/CTF records	5 years
Complaints records	7 years (or 5 years per CGA requirement)
Responsible Gaming records	5 years
Financial / transaction records	5 years (or longer per applicable law)
Employee records	Per employment law and AML requirements

13.6 Third-Party Data Processing

All third-party processors are subject to written data processing agreements that require them to:

- Process data only on the Company's documented instructions;
- Implement appropriate technical and organisational security measures;
- Not engage sub-processors without prior authorisation;
- Assist the Company in fulfilling data subject rights;
- Return or delete data upon termination of the agreement.

14. Marketing & Advertising Standards

14.1 General Principles

All marketing and advertising activities must be:

- Legal, decent, honest, and truthful;
- Compliant with CGA responsible gaming requirements;
- Not targeted at minors or vulnerable persons;
- Clearly identifiable as gambling advertising.

14.2 Prohibited Practices

- Depicting gambling as a way to generate income or solve financial problems;
- Implying that chance-based games can be influenced by skill or strategy;
- Targeting or using messaging that appeals to minors (including use of animated characters popular with children);
- Using sexual or explicit content;
- Associating gambling with alcohol, drugs, or harmful behaviours;
- Emotional manipulation — portraying gambling as a solution to stress or personal problems;
- Encouraging players to chase losses or gamble beyond their means.

14.3 Bonus & Promotions

- All bonus offers must clearly state their terms and conditions, including wagering requirements, expiry dates, game restrictions, and maximum withdrawal limits;
- Bonuses must not be designed to encourage irresponsible or excessive gambling;
- Bonuses are not offered to players who are self-excluded or in a cooling-off period;
- Deposit match bonuses and free spin promotions are clearly communicated without misleading "headline" offers.

14.4 Responsible Gaming Messaging

All gambling advertisements must prominently display a responsible gaming warning or slogan, such as: "Gamble Responsibly. 18+ only." or an equivalent CGA-approved message. Links to the Company's RG Section are included in digital marketing.

14.5 Affiliate Management

- All affiliate partners must sign an Affiliate Agreement that incorporates the Company's marketing standards and RG requirements;
- The Company actively monitors affiliate content to ensure compliance;
- Non-compliant affiliates are issued a notice to remediate; persistent non-compliance results in suspension or termination of the affiliate relationship;
- Affiliates are prohibited from targeting minors or placing advertisements on websites or platforms likely to appeal to minors.

14.6 Email & Direct Marketing

- All direct marketing is sent only to players who have opted in;

- Players can opt out of marketing at any time;
- Players in self-exclusion or cooling-off receive no marketing;
- Players who have exhibited signs of problem gambling are removed from promotional campaigns and not targeted with bonus offers.

15. Third-Party & Vendor Management

15.1 Scope

The Company engages the following categories of third parties:

- Platform Provider: Pragmatic Gaming Solutions (gaming platform and hosting);
- Gaming Content Providers: Pragmatic Play, Evolution, EGT, Amusnet, Hacksaw Gaming, Spribe;
- Aggregators: Hub88, Alea;
- Payment Processors: [To be completed];
- KYC/AML Technology Providers: [To be completed];
- ADR Provider: CADRE B.V.;
- Affiliates: Marketing partners.

15.2 Due Diligence

Prior to engagement, all material third parties are subject to due diligence including:

- Verification of legal status, ownership, and regulatory licences;
- Assessment of compliance posture (AML, data protection, information security, responsible gaming);
- Review of financial stability;
- Reference checks.

15.3 Contractual Requirements

All material third-party agreements must include provisions covering:

- Defined service levels (SLAs) and performance standards;
- AML/CTF compliance obligations and right-to-audit provisions;
- Data protection and confidentiality requirements;
- Information security standards (aligned with ISO/IEC 27001);
- Incident notification requirements (within 24 hours for material incidents);
- Compliance with CGA licence conditions applicable to the Company;
- Termination provisions including data return/deletion.

15.4 Ongoing Monitoring

- Third-party performance is reviewed at least annually;
- SLA compliance is monitored on an ongoing basis;
- Material incidents involving third parties are assessed and documented;
- Third parties that fail to meet contractual or compliance standards are subject to remediation plans or termination.

15.5 Critical Outsourcing (Platform Provider)

The Company's outsourcing of the gaming platform to Pragmatic Gaming Solutions is classified as critical outsourcing. Enhanced oversight applies:

- The Company retains full regulatory responsibility for all platform activities;
- The CGA is notified of the outsourcing arrangement and any material changes to it;
- The Platform Provider is subject to the Company's right-to-audit at all times;

- The Platform Provider maintains ISO/IEC 27001-aligned information security controls;
- Exit and contingency plans are maintained and tested annually.

16. Staff Recruitment, Screening & Training

16.1 Recruitment Standards

The Company recruits staff with appropriate qualifications, skills, and integrity. All candidates undergo a structured assessment process prior to appointment.

16.2 Pre-Employment Screening

All employees, contractors, and temporary staff who may have access to player data, financial transactions, or compliance processes are subject to:

- Criminal record check (via official Curaçao authorities or equivalent international channels);
- Financial integrity verification (credit check, bankruptcy/insolvency records, previous regulatory sanctions or AML-related disciplinary actions);
- Professional reference checks;
- Sanctions and PEP screening (to ensure no conflict with targeted financial sanctions);
- Right to work verification.

Individuals with relevant criminal convictions, financial misconduct, or regulatory sanctions that could compromise AML/CTF integrity will not be hired.

16.3 Ongoing Screening

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

16.4 Training Programme

16.4.1 AML/CTF Training

Audience	Training Content
All staff	ML/TF/PF awareness; red flags; no-tipping-off rules; Company policies
Customer-facing staff	Gambling-specific red flags; CDD request handling; customer interaction protocols
Compliance / MLRO / Risk	Advanced BRA/CRA; EDD; transaction monitoring; goAML reporting; PEP/sanctions; audit preparation
Senior management / Board	Oversight responsibilities; risk appetite; programme effectiveness; CGA reporting

AML/CTF training is:

- Initial: Completed as part of onboarding, before performing AML/CTF duties;
- Annual refresher: Mandatory for all staff;
- Ad-hoc: Upon new products/services, regulatory changes, or new ML/TF/PF typologies.

16.4.2 Responsible Gaming Training

All customer-facing and RG staff receive:

- Initial RG training during onboarding;

- Annual refresher;
- Training on: identifying gambling-related distress; sensitive player interactions; escalation procedures; use of RG tools.

16.4.3 General Compliance Training

All staff receive training on:

- Data protection and privacy;
- Information security (phishing, password hygiene, incident reporting);
- Complaints handling procedures;
- Code of conduct and ethics.

16.5 Training Records

A central training register is maintained, recording:

- Date and type of training;
- Training content and materials;
- Facilitator details;
- Assessment results and pass/fail status;
- Follow-up actions required.

Records are retained for at least five years and are available for CGA inspection. Non-completion of required training or failure to apply learned procedures may result in disciplinary action.

17. Regulatory Reporting & Record Keeping

17.1 CGA Portal Obligations

The Company maintains an active account on the CGA Licensee Portal (portal.gamingcontrolcuracao.org) and fulfils the following upload obligations:

Document	Frequency	Trigger
Operational Manual	Upon changes	Material change or annual review
AML/CTF/PF Policy	Upon changes	Material change or annual review
Responsible Gaming Policy	Upon changes	Material change or annual review
Complaints Policy	Upon changes	Material change or annual review
Financial reports	Per licence conditions	Periodic
Complaints data report	Bi-annually	6-monthly
RG effectiveness report	Annually	Annual

17.2 FIU Reporting

Unusual Transaction Reports (UTRs) and Suspicious Activity Reports (SARs) are submitted to the FIU Curaçao via the goAML portal by the MLRO:

- Without delay upon identification of reportable unusual transactions;
- Without tipping off the subject of the report.

17.3 Record Keeping Summary

Record Type	Minimum Retention
KYC / identity verification	5 years from end of relationship
AML/CTF records, transaction logs	5 years
UTRs / goAML submissions	5 years
Complaints records	7 years
Responsible Gaming records	5 years
Employee training records	5 years

All records are stored securely and are readily available for CGA or FIU inspection upon request.

18. Business Continuity & Disaster Recovery

18.1 Overview

The Company maintains business continuity and disaster recovery plans to ensure the resilience of gaming operations and the protection of player funds in the event of a disruption. The primary responsibility for technical disaster recovery lies with the Platform Provider (Pragmatic Gaming Solutions), which maintains separate disaster recovery measures as part of the outsourcing arrangement.

18.2 Business Continuity Planning

- Business continuity plans are maintained and tested at least annually;
- Risk and impact analyses are conducted to identify critical business functions and maximum tolerable downtime;
- Restoration procedures are documented for all critical systems;
- A single BCP framework ensures consistency across all business areas;
- Key staff are trained on BCP activation procedures.

18.3 Platform Provider Obligations

The Platform Provider must:

- Maintain a production environment with redundancy and failover capabilities;
- Conduct regular disaster recovery testing;
- Achieve defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) as specified in the SLA;
- Notify the Company within 24 hours of any incident affecting platform availability.

18.4 Player Fund Protection

In the event of business disruption or insolvency:

- Player funds held in segregated accounts are protected;
- The Company will communicate promptly with affected players and the CGA regarding fund availability and recovery;
- No player funds are used for Company operational expenses.

18.5 Regulatory Notification

The CGA is notified immediately of any material operational disruption that affects:

- The availability of gaming services to players;
- Player fund security;
- The Company's ability to fulfil regulatory obligations.

19. Anti-Fraud & Game Integrity

19.1 Anti-Fraud Framework

19.1.1 Fraud Detection

- Automated fraud detection rules integrated into the gaming platform and payment systems;
- Real-time monitoring for suspicious patterns including: multi-accounting, bonus abuse, chargebacks, identity fraud, collusion, and chip dumping;
- Device fingerprinting and IP monitoring to detect duplicate accounts and VPN/proxy use from restricted jurisdictions.

19.1.2 Bonus Abuse

- Bonus terms and conditions are clearly stated and enforced;
- Abuse of bonuses (e.g., through multi-accounting or deliberate exploitation of terms) may result in account suspension, forfeiture of bonus funds and associated winnings, and permanent account closure.

19.1.3 Chargeback Fraud

- Accounts subject to chargebacks are reviewed by the Payments and Compliance teams;
- Confirmed chargeback fraud results in account suspension and potential blacklisting;
- The Company co-operates with payment processors and card networks to manage and dispute fraudulent chargebacks.

19.2 Sports Betting Integrity

- The Company monitors sportsbook activity for patterns indicative of match-fixing, suspicious betting, or insider information;
- The Company reserves the right to void bets where there is credible evidence of match manipulation;
- The Company co-operates with relevant sporting integrity bodies and authorities in relation to any suspected manipulation;
- Suspicious betting reports are escalated to the Compliance Officer for assessment.

19.3 Account Takeover Prevention

- Players are encouraged to use strong, unique passwords and to enable MFA;
- Unusual login activity (new device, new IP, new country) triggers security alerts to the player;
- Accounts with suspected takeover are frozen pending verification.

19.4 Self-Exclusion Cross-Check

The Company screens all new registrations against its internal self-exclusion database to prevent excluded players from creating new accounts. Accounts identified as belonging to self-excluded players are closed immediately and any deposits refunded.

20. Policy Review & Document Control

20.1 Review Schedule

This Operational Manual is subject to:

- Annual review: At minimum, reviewed and updated once every calendar year;

Event-triggered review: Immediate review upon:

- Material changes to the LOK or CGA regulations;
- Significant changes to the Company's business (new products, markets, personnel, or providers);
- Material findings from audits, inspections, or regulatory feedback;
- Any serious incident or near-miss affecting compliance.

20.2 Approval Process

All revisions to this Manual require:

25. Drafting of proposed amendments by the Compliance Officer;
26. Legal/regulatory review;
27. Presentation to the Board of Directors;
28. Board approval and sign-off;
29. Upload to the CGA Licensee Portal within the required timeframe;
30. Distribution to all relevant staff.

20.3 Version Control

All versions of this Manual are version-controlled. The version history is maintained in the Version Control table at the front of this document. Previous versions are archived securely for a minimum of five years.

20.4 Staff Acknowledgement

Upon issue of a new version of this Manual:

- All employees receive a copy or notification of access;
- All employees complete a mandatory acknowledgement confirming they have read, understood, and agree to comply with the Manual;
- The Compliance Officer maintains a central register of all acknowledgements;
- Non-compliance with this Manual may result in disciplinary action up to and including termination.

20.5 Document Storage

This Manual and all associated policies, review documentation, Board approvals, and staff acknowledgements are stored securely and are available for CGA inspection at all times.

Appendices

Appendix A: Regulatory Reference List

- 31. National Ordinance on Games of Chance (Landsverordening op de kansspelen — LOK), PB 2024, no. 157 (effective 24 December 2024)
- 32. CGA Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction, Version January 10, 2025
- 33. National Ordinance on Identification when Rendering Services (LID)
- 34. National Ordinance on the Reporting of Unusual Transactions (LMOT)
- 35. CGA Responsible Gaming Policy, Version 1.0, 17 April 2025 (post-consultation final)
- 36. CGA Player Complaints Policy Guidelines, Version 1.1, 18 June 2025
- 37. CGA Alternative Dispute Resolution (ADR) Role and Certification Guidelines, Version 1.0, 8 September 2025
- 38. CGA Online Portal User's Manual (updated January 2026)
- 39. Kingdom of the Netherlands Sanctions Act (Sanctiewet 1977)
- 40. FATF 40 Recommendations (as applicable to online gaming operators)
- 41. CFATF Guidance for Online Gaming Operators
- 42. ISO/IEC 27001:2022 Information Security Management Systems

Appendix B: Key Contacts

Role	Name	Contact
Compliance Officer	Nicholas Gatt	Nicholas Gatt
ADR Provider	CADRE B.V.	www.cadre.online
CGA	Curaçao Gaming Authority	www.gamingcontrolcuracao.org
FIU Curaçao	Financial Intelligence Unit	goAML portal

Appendix C: Glossary of Key Terms

ADR: Alternative Dispute Resolution — an independent process for resolving disputes between players and the operator.

AML: Anti-Money Laundering.

BRA: Business Risk Assessment — enterprise-wide assessment of ML/TF/PF risks.

CADRE B.V.: Curaçao Alternative Dispute Resolution Entity — the Company's CGA-certified ADR provider.

CAP: Customer Acceptance Policy — defines which customers can be accepted and under what conditions.

CDD: Customer Due Diligence — identification, verification, and ongoing monitoring of customers.

CGA: Curaçao Gaming Authority — the regulator.

CPF / PF: Countering Proliferation Financing / Proliferation Financing.

CRA: Customer Risk Assessment — player-specific ML/TF/PF risk evaluation.

CTF: Countering the Financing of Terrorism.

DPO: Data Protection Officer.

EDD: Enhanced Due Diligence — additional CDD measures for high-risk scenarios.

FATF: Financial Action Task Force — international standard-setter for AML/CTF.

FIU: Financial Intelligence Unit — Curaçao's financial intelligence authority.

GGR: Gross Gaming Revenue.

goAML: The FIU Curaçao's secure portal for reporting unusual or suspicious transactions.

KYC: Know Your Customer.

LID: National Ordinance on Identification when Rendering Services.

LMOT: National Ordinance on the Reporting of Unusual Transactions.

LOK: Landsverordening op de kansspelen — National Ordinance on Games of Chance.

ML: Money Laundering.

MLRO: Money Laundering Reporting Officer.

MFA: Multi-Factor Authentication.

NAf: Netherlands Antillean Florin — Curaçao's local currency.

PEP: Politically Exposed Person.

RG: Responsible Gaming.

RGO: Responsible Gaming Officer.

RNG: Random Number Generator.

RTP: Return to Player — the percentage of wagered funds returned to players over time.

SDD: Simplified Due Diligence.

SLA: Service Level Agreement.

TF: Terrorist Financing.

UTR: Unusual Transaction Report.

Appendix D: Restricted Jurisdictions Policy

The Company maintains an internal list of jurisdictions from which it does not accept players. This list is based on:

- FATF High-Risk Jurisdictions subject to a Call for Action;
- FATF Jurisdictions under Increased Monitoring ("grey list");
- CFATF Public Statement jurisdictions;
- EU list of non-cooperative jurisdictions for tax purposes;
- OFAC sanctioned countries;
- Countries subject to CGA guidance;
- Countries where online gambling is illegal for the operator to provide services.

The Restricted Jurisdictions List is maintained by the Compliance Officer, reviewed quarterly, and updated immediately upon any changes to the above reference lists. Geolocation technology blocks access from restricted jurisdictions at both registration and login.
