

OPERATIONAL MANUAL

COMPLIANCE FRAMEWORK PURSUANT TO THE NATIONAL ORDINANCE ON GAMES OF CHANCE (LOK)

OPERATOR / LICENSEE: GBL Solutions N.V.
EFFECTIVE DATE: 10.06.2026 / Version 1.0

PREAMBLE

WHEREAS, GBL Solutions N.V. (hereinafter referred to as the "Licensee"), managing and directing online gaming brands (hereinafter collectively referred to as the "Website(s)" or "Platform(s)"), has developed this Operational Manual to strictly reflect its core operational policies, internal corporate protocols, and technical security architecture;

WHEREAS, this instrument is meticulously drafted in strict compliance with the statutory and regulatory requirements set forth under Article 5.9, paragraph 1, letters (a) through (j) of the National Ordinance on Games of Chance (LOK) of Curaçao; and

WHEREAS, the primary objective of this Manual is to provide the Curaçao Gaming Authority (hereinafter "CGA") and all relevant regulatory stakeholders with a transparent, verifiable, and comprehensive structural overview of the Licensee's multi-brand gaming operations, ensuring the absolute safeguarding of players, financial integrity, and systemic infrastructure;

NOW, THEREFORE, the Licensee hereby formally establishes, implements, and binds its operations to the following formal operational and compliance framework:

ARTICLE 1: GAMES OF CHANCE, PAYMENTS, AND SOFTWARE SPECIFICATIONS

Section 1.1. Scope of Games Offered. The Licensee shall offer a comprehensive and legally compliant portfolio of games of chance across its Website(s). This portfolio encompasses video slots, Random Number Generator (RNG) table games (including, but not limited to, Roulette, Blackjack, Baccarat, and Poker), and specialized Live Casino environments featuring real-time dealers. All interactive gaming products shall be sourced exclusively from licensed, audited, and top-tier B2B software suppliers.

Section 1.2. Payment Processing and Gateways. The Licensee shall maintain secure, diverse, and heavily encrypted payment pathways for end-users across all active brands. Supported financial mechanisms shall facilitate transactions via internationally recognized credit/debit cards, certified electronic wallets, secure electronic wire transfers, and authorized cryptocurrency gateways supporting prominent digital assets.

For certain payment processing activities, the Licensee utilizes Payment Agent Services.

The Licensee maintains arrangements designed to ensure the segregation of player funds from operational funds. Client funds are held separately from funds used for operational expenses, salaries, commissions, taxes and other business obligations.

Player funds may be maintained either directly by the Licensee or through the Payment Agent exclusively for the benefit of players and in accordance with the Licensee's Segregation Policy.

Payment transactions are processed through a combination of approved Payment Service Providers (PSPs), banking institutions, Electronic Money Institutions (EMIs) and cryptocurrency payment solutions. All payment providers are subject to appropriate due diligence and ongoing monitoring procedures.

Section 1.3. Wagering Limits and RTP Disclosures. Minimum and maximum betting parameters shall be configured dynamically on a per-game and per-brand basis, with entry-level stakes starting as low as 0.10 EUR and maximum limits scaling up appropriately to accommodate high-roller segments at VIP tables. The theoretical Return to Player (RTP) percentages must remain conspicuously displayed

and accessible within the informational interface of each respective game software to ensure absolute transparency.

Section 1.4. Software Integrity and RNG Protocols. With the deliberate exception of live dealer environments, the complete fairness, unpredictability, and mathematical randomness of all game outcomes shall be governed strictly by a certified and un-tamperable Random Number Generator (RNG). The Licensee's centralized secure platform architecture shall execute real-time management of player financial balances and seamlessly interface with gaming systems via an encrypted Application Programming Interface (API).

Section 1.5. Gaming Platform and Content Providers. The Licensee conducts its gaming operations through the gaming platform, which provides the core gaming infrastructure, player account management functionality, transaction processing interfaces and gaming integrations.

The Licensee offers online casino, sports betting, poker and bingo products through the platform.

Gaming content is supplied through a network of licensed third-party game providers integrated via the platform. The Licensee maintains a register of game providers and applicable certifications and shall make such records available to the Curaçao Gaming Authority upon request.

All RNG-based games offered by the Licensee are subject to certification requirements maintained by the relevant suppliers and platform provider. Records of RNG certifications are retained by the Licensee in accordance with its record-keeping obligations.

ARTICLE 2: QUALITY MONITORING AND PERIODIC SYSTEM TESTING

Section 2.1. Quality and Compliance Auditing. The Licensee shall subject its unified technical platform architecture to non-disruptive, continuous monitoring protocols to guarantee high-availability operational stability. Mandatory quality audits and strict RNG testing shall be executed at minimum on an annual basis by globally recognized, accredited independent testing laboratories.

Section 2.2. Vulnerability Management and Penetration Testing. The Licensee's designated technical operations division shall oversee the execution of comprehensive, bi-annual penetration testing (Penetration Testing) managed by certified external cyber-security firms. Furthermore, automated defensive scripts shall be deployed daily to perform comprehensive vulnerability assessments and neutralize emerging malware threats.

ARTICLE 3: DATA RETENTION, ARCHIVING, AND PRIVACY STANDARDS

Section 3.1. General Confidentiality Framework. The handling, processing, and storage of player data shall be strictly governed by a rigid corporate confidentiality protocol aligned with global data protection standards. All personally identifiable information (PII) and related sensitive financial history shall be housed exclusively on production servers heavily shielded by multi-layered next-generation firewalls.

Section 3.2. Strict Data Encryption Standards. The Licensee mandates the systematic enforcement of bank-grade cryptographic protocols. This explicitly requires the application of Advanced Encryption Standard (AES)-256 bit encryption for all data at-rest, and Transport Layer Security (TLS) 1.3 encryption for all data in-transit across public and private networks.

Section 3.3. Access Controls and Statutory Retention Periods. Internal technical and operational access to database environments containing player data shall be strictly restricted via Role-Based Access Controls (RBAC), completely logged for auditing purposes, and authorized solely on a verified

"need-to-know" basis. Data retention schedules shall fully satisfy international Anti-Money Laundering (AML) directives and regional statutory preservation requirements.

ARTICLE 4: USER INTERFACE ARCHITECTURE AND VISUAL DISCLOSURES

Section 4.1. Visual and UI Transparency. The structural layout of the user interface (UI) deployed across the Licensee's operational Website(s) shall be designed to foster an honest, informative, and entirely non-misleading user environment. Information delivery must be clear and readily accessible.

Section 4.2. Mandatory Constant Screen Disclosures. The underlying platform software shall ensure that the following baseline metrics and navigational links remain clearly visible on the player's viewable screen space at all times during an active gaming session:

- The real-time available account balance, clearly bifurcated into withdrawable real/fiat/crypto funds and restricted promotional bonus balances;
- The precise active wager amount per round and the immediate corresponding winning disbursement values;
- An ongoing session clock serving as a mandatory "Reality Check" feature to optimize temporal awareness and prevent excessive play;
- Highly visible and direct hyperlinks navigating instantly to the dedicated Responsible Gaming module and the corporate General Terms & Conditions.

ARTICLE 5: ADMISSION PREVENTION AND TECHNICAL ENTRY BLOCKING

Section 5.1. Regulatory KYC Protocols. The Licensee shall enforce mandatory, multi-tiered Know Your Customer (KYC) identity verification procedures deeply embedded into the account onboarding, deposit, and withdrawal operational workflows.

Section 5.2. Automated Systematic Blocking Criteria. The structural systems governing the platforms shall automatically deny system access, terminate connections, or prevent account generation under the following criteria:

- Any individual failing to substantiate the legal gambling age threshold of 18 years of age (enforced via strict Date of Birth algorithm checks and document verification);
- Inbound connections originating from Internet Protocol (IP) addresses mapped to legally restricted, blacklisted, or prohibited jurisdictions via automated Geo-IP blocking technologies;
- Users registered within the database's internal central Self-Exclusion system or synchronized with external national databases of prohibited persons;
- Individuals flagged on global Sanctions lists (OFAC, UN, EU) or categorized as high-risk Politically Exposed Persons (PEPs) via persistent, automated tier-1 API screening integration workflows.

ARTICLE 6: TECHNICAL INFRASTRUCTURE AND DISASTER RECOVERY SYSTEMS

Section 6.1. Logic Architecture and DDoS Defense. The Licensee's production infrastructure shall utilize a redundant, distributed tier architecture, segregating web application front-ends, core transactional database clusters, and secure storage layers (Data Vault). Public-facing endpoints shall be actively defended by enterprise-grade, high-capacity anti-DDoS mitigation services.

Section 6.2. Disaster Recovery Plan (DRP) and Operational Objectives. Operational and database records shall be replicated synchronously across geographically separated, secure data centers. In the

catastrophic event of primary infrastructure failure, the DRP mandates a Recovery Time Objective (RTO) not to exceed a maximum of 4 hours, and a targeted Recovery Point Objective (RPO) of 0-5 minutes, successfully preserving all transactional and financial data without discrepancy.

ARTICLE 7: RESPONSIBLE GAMING PRINCIPLES IMPLEMENTATION

Section 7.1. Corporate Commitment to Player Protection. Pursuant to the mandatory statutory obligations delineated within Article 2.2 paragraph 3, Article 5.4, and Article 5.6 of the National Ordinance on Games of Chance (LOK), the Licensee shall position player welfare and harm minimization as core components of its operational philosophy across all brands.

Section 7.2. Integrated Responsible Gaming Mechanisms. The underlying software engine across the Website(s) shall empower end-users with accessible, self-administered player-protection parameters within their secure profile dashboards, precisely including:

- Cooling-Off / Time-Out Status: Immediate provisions enabling temporary suspension of account interaction capability spanning from 24 hours up to several calendar months;
- Definitive Self-Exclusion: An absolute and irrevocable system block terminating profile access for a specified prolonged duration or an indefinite period;

Section 7.3. Behaviour Monitoring and Intervention. The Licensee maintains procedures for identifying and responding to indicators of potentially harmful gambling behaviour in accordance with its Responsible Gaming Policy.

Behaviour monitoring may be conducted through trained personnel and supported by technological systems where appropriate.

Where indicators of concern are identified, the Licensee may undertake responsible gaming interventions including responsible gaming communications, account reviews, temporary suspensions, self-exclusion measures and other protective actions deemed appropriate under the circumstances.

Section 7.4. Responsible Gaming Record Keeping. The Licensee maintains records of responsible gaming interactions, player requests, interventions and actions taken in accordance with its Responsible Gaming Policy and applicable regulatory requirements.

Responsible gaming records are retained and made available to competent authorities where required by law.

ARTICLE 8: GENERAL TERMS AND CONDITIONS STANDARDS

Section 8.1. Binding Legal Consensus. The legal, contractual, and binding framework regulating all interactive relations between the Licensee and the consumer shall be governed exclusively by the prevailing version of the General Terms and Conditions (T&C) specific to each respective gaming Website.

Section 8.2. Holistic Integration of Internal Policies. The T&C, located permanently and accessibly within the footer navigation of the respective Website(s), shall structurally incorporate by reference the general casino rules, the corporate AML policy, the privacy policy, standard promotional bonus rules, and the financial guidelines governing withdrawal mechanics. Explicit user acceptance of these terms is an un-waivable prerequisite for successful account validation.

ARTICLE 9: COMPLAINT HANDLING AND DISPUTE RESOLUTION PROTOCOLS

Section 9.1. Formal Dispute Resolution Architecture. In strict conformity with the dispute tracking and administrative mandates defined by Article 5.3 of the LOK, the Licensee shall institute and fund a structured, three-tier dispute escalation mechanism:

1. Tier 1 (Initial Intake): The consumer shall formally transmit their grievance or dispute file directly to the dedicated Customer Support department via the active support email channel of the specific Website or via the Live Chat application.
2. Tier 2 (Internal Escalation): Should the underlying dispute fail to reach a mutually satisfactory resolution within a commercially reasonable timeframe, the case file shall be formally transferred to the designated internal Compliance Officer or Casino General Manager for independent administrative review.
3. Tier 3 (External Escalation & ADR): Upon complete exhaustion of internal corporate remedies without reaching consensus, the Licensee shall formally notify the user of their unconditional legal right to submit the matter, entirely free of charge, to an independent approved Alternative Dispute Resolution (ADR) body or escalate the matter directly to the Curaçao Gaming Authority (CGA).

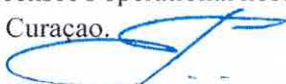
ARTICLE 10: MANDATORY DIGITAL RECORD-KEEPING AND SEVERE DATA VAULT OVERVIEW

Section 10.1. Data Vault Functional Infrastructure. To fully satisfy the ongoing technical control, real-time tracking, and administrative oversight mandates dictated by the CGA under the LOK, the Licensee shall continuously maintain an independent "Data Vault" infrastructure. This software layer must automatically, instantly, and immutably capture and archive critical operational parameters across all operating brands, explicitly including:

- Comprehensive verified player profile registries, inclusive of complete KYC validation metadata and uploaded identity documentation history;
- Detailed historical gaming logs, comprehensively tracking every individual wager placed, software spin, game round outcome, session connection, and corresponding payout calculation;
- Complete financial ledgers documenting the source, destination, routing, and processing state of all monetary transactions (deposits, transfers, and withdrawals).

Section 10.2. Tier-IV Certified Curaçao Server Infrastructure. All operational and transactional logs aggregated under Section 10.1 shall be permanently archived in a structurally immutable, write-once-read-many (WORM) format on a physical, dedicated server array housed strictly within an officially registered, Tier-IV certified Data Center located territorially within the physical jurisdiction of Curaçao. This dedicated infrastructure shall remain configured to grant uninterrupted, secure, and immediate data-extraction capabilities to authorized officials of the Curaçao Gaming Authority (CGA) at all times, thereby assuring complete transparency and perfect regulatory alignment with the National Ordinance.

Section 10.3. Hosting and Operational Environment. The Data Vault infrastructure forms part of the Licensee's operational hosting environment maintained within the Tier-IV certified data centre operated in Curaçao.



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

Managing Director

26.06.2026