

Operations Manual

Operator: JarvisDelivery B.V.

License Number: OGL/2024/244/0341

Jurisdiction: Curaçao

Date of implementation: September 01, 2025

Status: Approved

This Operations Manual has been prepared in accordance with Article 5.9 of the National Ordinance on Games of Chance and the rules and requirements imposed by the Curaçao Gaming Authority (CGA).

Its purpose is to:

- Document the manner and degree of compliance with the National Ordinance and licensing conditions.
- Provide a transparent and auditable reference for the CGA, stakeholders, and internal staff.
- Ensure that all aspects of the licensed operations, including games offered, technical infrastructure, data security, responsible gaming, and dispute resolution, are clearly defined, maintained, and monitored.

This manual is a living document and shall be:

- Maintained at all times by the Operator.
- Reviewed annually or earlier in case of significant operational or regulatory changes.
- Updated versions will be submitted to the CGA as required.

1. Games of Chance Description

Portfolio: Online casino (slots, table games, live dealer), sportsbook, and RNG-based games.

Operations: Games are delivered through licensed third-party providers integrated via secure APIs. All third-party providers before integrating with the Company share the relevant RNG certificate and the latest Gaming Test Reports (in accordance with the GLI 19 standard).

Payment Options: Credit/debit cards, bank transfers, e-wallets, and approved cryptocurrencies.

Betting Limits: Min €0.10 per bet; Max €5,000 per transaction (configurable by game type).

Payouts: Payouts via PSPs, with specific limits per day/week/month in accordance with the Terms and Conditions.

Software: RNG games tested and certified by BMM Testlabs/GLI and other approved laboratories.

Outcome Determination: RNG certification + audited odds, monitored by internal compliance.

2. Test Methods for Quality Monitoring

The Operator implements a structured Quality Assurance (QA) and Testing Framework to ensure continuous compliance with licensing requirements, fair play, system integrity, and player protection. The following measures apply:

2.1. RNG Testing and Certification

All Random Number Generator (RNG) software used in casino games, slots, and table games is tested by an independent accredited laboratory (e.g., GLI, BMM Testlabs, eCOGRA).

RNG certifications are renewed annually or immediately after significant software updates.

Certificates are maintained in the Operator's compliance register and made available to the Curaçao Gaming Authority (CGA) upon request.

A sample of game rounds is periodically validated internally against RNG outputs to confirm alignment with the certified random distribution.

2.2. Game Fairness and RTP (Return-to-Player) Verification

All games display their theoretical RTP values in compliance with fair gaming standards.

The Operator performs monthly RTP verification using aggregated gameplay data, comparing actual vs. theoretical RTP. Any discrepancy beyond $\pm 1\%$ is flagged, investigated, and escalated to the Compliance Officer.

Reports are retained for five years and made available during CGA audits.

2.3. Payment Flow and Transaction Reconciliation

Weekly reconciliation between the Operator's platform data and PSP/acquirer settlement reports is performed by the Finance Team. Variances in deposits, withdrawals, chargebacks, or refunds greater than 0.5% trigger investigation.

A reconciliation log (with variance explanations) is stored securely for five years in line with AML/CTF record-keeping requirements. Monthly compliance reports include reconciliation summaries for review by management.

2.4. Penetration Testing & Cybersecurity Assessments

Quarterly penetration tests are performed by external cybersecurity providers certified under CREST/ISO 27001 standards. Tests include network, application, and API layers, as well as vulnerability scans for payment integrations. Critical or high vulnerabilities must be remediated within 7 business days, with retesting required.

Results are reviewed by the Compliance and IT Security teams, and remediation evidence is logged. An annual Red Team exercise is conducted to simulate real-world attacks, including phishing and social engineering.

2.5. Change Management Testing

Any new software release, patch, or system update undergoes staging environment testing before deployment.

Tests include functionality, regression, security scanning, and load/stress testing. A change approval board (CAB) signs off on deployments with compliance oversight.

2.6. Business Continuity & Disaster Recovery Drills

Twice per year, a disaster recovery (DR) simulation is conducted to ensure platform resilience.

Recovery Time Objective (RTO) and Recovery Point Objective (RPO) are tested against set benchmarks (e.g., $RTO \leq 4$ hours). Results are documented and shared with management.

2.7. Player Account & AML Testing

Monthly testing of KYC workflows is performed using test accounts to validate document verification, source-of-funds checks, and age verification.

AML monitoring rules are tested quarterly (e.g., structuring, rapid deposits/withdrawals, use of high-risk payment methods).

Compliance team reviews flagged cases to confirm monitoring thresholds are working as intended.

2.8. Reporting & Escalation

A Quality Monitoring Report is produced quarterly summarizing:

- RNG certification status,
- RTP verification outcomes,
- Payment reconciliation summaries,
- Penetration test and remediation results,
- Compliance testing logs.

The Compliance Officer escalates unresolved issues to the Board and, where required, notifies the CGA.

3. Player Data Storage

3.1. PII Storage

All personally identifiable information (PII) is stored using AES-256 encryption at rest and secured during transmission with TLS 1.2/1.3. Data is hosted in a Tier-IV certified data center located in Curaçao, ensuring redundancy, uptime, and regulatory alignment. Regular integrity checks and encryption key rotations are performed to maintain security.

3.2. Access Control

Access to PII is strictly role-based and granted only to compliance staff and authorized technical personnel on a “need-to-know” basis. All access attempts are logged and subject to monthly audit reviews by the Compliance Officer. Multi-factor authentication (MFA) is enforced for all privileged accounts.

3.3. Retention Period

PII and KYC records are retained for a minimum of five (5) years after account closure, in line with Curaçao’s AML/CFT record-keeping obligations. After expiry of the retention period, data is either securely deleted or anonymized, unless longer storage is legally required. Players are informed of retention practices in the Privacy Policy.

3.4. GDPR Rights and Compliance

The Operator is committed to protecting personal data in accordance with the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and applicable data protection laws. The following procedures ensure that all data subject rights are respected, processed without undue delay, and recorded for audit purposes.

3.4.1. Right of Access (Article 15 GDPR)

Players may submit a “Data Access Request” via the Support Center or Compliance email. The Operator will verify the player’s identity (KYC match + security questions) before disclosing data. A copy of all personal data held will be provided within 30 days of receipt of a valid request. Response includes categories of data processed, purposes, recipients, storage periods, and legal bases.

3.4.2. Right to Rectification (Article 16 GDPR)

Players may request corrections to inaccurate or incomplete personal data. Rectification requests are handled within 14 days after verification of identity. Audit trail maintained showing the original and corrected data.

3.4.3. Right to Erasure (“Right to be Forgotten”, Article 17 GDPR)

Players may request deletion of their personal data. Requests will be honored where no overriding legal/regulatory obligation requires retention (e.g., AML/CFT rules require retention for minimum 5 years). If deletion is restricted, the Operator will anonymize the data where possible and notify the player.

3.4.4. Right to Restrict Processing (Article 18 GDPR)

Players may request suspension of processing in specific circumstances (e.g., contesting accuracy, pending investigation). The Operator will mark the account as “restricted” and freeze processing, except as required for regulatory/legal purposes.

3.4.5. Right to Data Portability (Article 20 GDPR)

Players may request a machine-readable copy of their personal data (CSV, JSON). Provided within 30 days and transmitted directly to another controller upon player request, subject to technical feasibility.

3.4.6. Right to Object (Article 21 GDPR)

Players may object to processing based on legitimate interest (e.g., marketing). Marketing communications immediately suppressed upon objection. Gaming-related compliance processing (AML, fraud prevention) cannot be suppressed.

3.4.7. Automated Decision-Making & Profiling (Article 22 GDPR)

The Operator does not engage in solely automated decision-making with legal effects. Any risk-based profiling (e.g., AML monitoring, responsible gaming alerts) is subject to human oversight.

3.4.8. Submitting & Tracking Requests

Requests can be made via:

- Player Account dashboard (“Privacy Settings”),
- Email to support@flexy-spin.com, or
- Written notice to the Compliance Department (registered office address).

All requests logged in the Data Subject Request Register, maintained by the Data Protection Officer (DPO) / Compliance Officer. Register includes date received, identity verification performed, deadline, outcome, and responsible handler.

3.4.9. Escalation & Oversight

The Compliance team handles operational requests. The Legal team oversees complex cases (e.g., conflicts with AML obligations). DPO/Compliance Officer reviews all requests monthly to ensure timelines and obligations are met.

3.4.10. Player Communication

All responses must be clear, transparent, and in plain language. Denials (e.g., erasure blocked due to AML) must be justified in writing and reference the relevant legal basis.

4. Visual Elements to Players

4.1. Responsible Gaming Messages

Messages and reminders about responsible play are displayed at login and at set intervals during gameplay sessions. Links to external support organizations (e.g., GamCare, Gambling Therapy) are always visible. Pop-up reminders appear if session duration or betting thresholds are exceeded.

4.2. Account Balance

Players can see their real-time account balance (cash, bonus, and coin balances separately) at all times. Balances are updated instantly after every bet, win, deposit, or withdrawal.

4.3. Deposit Limits

Deposit limits are clearly displayed in the cashier interface. Players are reminded of their daily, weekly, and monthly limits when making a deposit. Any request to raise limits triggers a mandatory 24-hour cooling-off period.

4.4. Terms and Conditions

Full Terms and Conditions are linked in the website footer and during the registration process. Players must actively confirm acceptance of the Terms before account creation. Updates to Terms are notified by in-account messaging and email.

4.5. Fair Play and RNG Certificate

A Fair Play statement is displayed in the footer and Help section, affirming game fairness and transparency. Reference to the Operator's independent RNG certification (e.g., GLI/BMM) is provided with certificate details available on request.

5. Technical Measures to Prevent Banned Persons

5.1. Geoblocking

Access from prohibited or restricted jurisdictions is blocked using IP-based geolocation technology. The system automatically detects and prevents login, registration, and gameplay from banned regions. VPN/proxy detection tools are applied to reduce circumvention attempts.

5.2. Self-Exclusion Tools

Players can request temporary or permanent exclusion through their account settings or by contacting support. Excluded accounts are immediately locked and flagged in the system to prevent reactivation. Self-exclusion requests are binding and cannot be reversed before the chosen period expires.

5.3. Watchlist Screening

All players are continuously screened against the Curaçao Gaming Authority's banned list and the Operator's internal exclusion list. Matches automatically trigger an account freeze pending compliance review. Watchlist screening is updated in real time through automated monitoring tools.

5.4. Underage Prevention

No withdrawals are processed until full KYC verification confirms the player is at least 18 years old. Identity documents are validated through manual and automated checks. Suspicious or forged documents result in immediate account suspension and reporting to the Compliance team.

6. Technical Infrastructure & Emergency Restoration

6.1. Hosting

The primary platform infrastructure is hosted in a Tier-IV certified data center in Curaçao, ensuring maximum uptime, redundancy, and compliance with local hosting requirements. A secondary backup environment is maintained on AWS (EU region) to provide geographical diversity and resilience. Data replication occurs in near real time between the primary and secondary sites.

6.2. Disaster Recovery (DR) Parameters

Recovery Point Objective (RPO): 24 hours – no more than 24 hours of data can be lost in the event of a disruption.

Recovery Time Objective (RTO): 48 hours – services must be restored within 48 hours of a declared incident.

Critical systems (payment processing, player balances, and RNG services) are prioritized for restoration.

6.3. Failover & Redundancy

The system uses redundant servers with automated real-time replication for critical services (databases, game engines, cashier). Failover procedures are designed to activate automatically, ensuring minimal downtime. Load balancing mechanisms distribute traffic to maintain performance during high demand or partial outages.

6.4. Emergency Procedures & Testing

Disaster Recovery drills are conducted twice annually, simulating system failure and full recovery scenarios. Test results are documented, and corrective actions are implemented where recovery times or processes fall short. Emergency contacts and escalation protocols are maintained, with a 24/7 technical support team on standby.

7. Responsible Gaming Implementation

7.1. Tools Available to Players

Players have access to a full suite of responsible gaming tools directly from their account dashboard and cashier. Available options include:

- Deposit limits (daily, weekly, monthly) configurable by the player.
- Wagering limits to restrict the total bet amount over a set period.
- Session limits and time-out options allowing temporary breaks from play.
- Self-exclusion options ranging from 12 months to permanent exclusion.

All limit increases are subject to a 24-hour cooling-off period; limit decreases apply immediately.

7.2. Monitoring

Automated risk monitoring tools track player activity patterns in real time, including:

- Unusually rapid deposits or repeated failed deposit attempts.
- High or escalating losses within a short period.
- Extended playing sessions beyond responsible thresholds.

Alerts are reviewed by the Compliance/Anti-Fraud teams, who decide on appropriate intervention.

7.3. Intervention

Customer Support agents and Responsible Gaming officers receive specialized training on identifying and addressing signs of problem gambling. Interventions may include:

- Sending automated or personalized warning messages.
- Temporarily restricting the player's account until further checks are completed.

- Encouraging the player to use available responsible gaming tools.

In severe cases, enforcing exclusion and referring the player to support services.

7.4. Education

A dedicated Responsible Gaming Information Page is available in the Help section and at registration. The page includes:

- Information about healthy gambling habits.
- Self-assessment questionnaires to identify risky behavior.
- Links to recognized NGOs and support organizations such as GamCare, Gambling Therapy, and Gamblers Anonymous.

Players are reminded of responsible gaming principles in regular account communications and during long sessions.

8. General Terms and Conditions

Most recent T&Cs are published on the website and reviewed annually. Cover eligibility (18+), restricted jurisdictions, deposit/withdrawal policies, dispute resolution, and AML obligations.

Players must accept updated T&Cs at first login after revision.

9. Dispute Resolution

Internal procedure:

Step 1: Complaint submitted to Customer Support.

Step 2: Escalation to Compliance Officer if unresolved within 14 days.

External ADR: If unresolved internally, referred to EGIS FZCO (or other CGA-approved ADR).

Documentation: All dispute records retained for 5 years and available to CGA upon request.

10. Digital Records & Data Center Requirement

Records kept:

- Player profiles, registration details, KYC data.
- Game transactions (bets, wins, losses).
- Financial transactions (deposits, withdrawals, chargebacks).

Storage location: Maintained at all times in a Tier-IV certified data center in Curaçao.

Format: Encrypted, indexed, and retrievable upon CGA request within 48 hours.

11. Permanent Education & Training

In accordance with Article 5.9(4) of the National Ordinance on Games of Chance (LOK), the Operator is committed to providing ongoing, annual training and education for all Support, Anti-Fraud, Marketing, Compliance and Legal personnel working in the field of Games of Chance under this license.

11.1. Scope of Training

Training programs will cover, at a minimum, the following topics:

- Mental well-being – awareness of stress, burnout, and mental health for both employees and players.
- Anti-bribery and corruption – policies and practical scenarios to prevent bribery in business operations.

- Crime prevention – procedures to identify and mitigate risks of fraud, collusion, and system abuse.
- Responsible gaming – awareness of tools, early warning signs of problem gambling, and escalation protocols.
- Anti-money laundering (AML/CFT) – training on customer due diligence, transaction monitoring, and reporting obligations.
- Communication with players – responsible, transparent, and respectful engagement.
- Responsible advertising – ensuring that marketing practices are socially responsible and compliant with regulatory standards.

11.2. Frequency

Training will be conducted on an annual basis and repeated as required when new risks, regulations, or technologies emerge. New employees must complete induction training within their first 30 days.

11.3. Documentation & Records

Attendance records, training content, and assessment results will be maintained for at least five (5) years. Records will be made available to the Curaçao Gaming Authority (CGA) upon request.

The Compliance Officer ensures training programs are updated annually. The Top Management reviews and approves the training plan and confirms regulatory compliance.

12. Compliance & Accountability

This Operations Manual reflects the Operator's commitment to regulatory compliance, fair gaming, player protection, and data security. All employees, contractors, and partners are expected to comply with the procedures outlined herein.

The Compliance Officer is responsible for ensuring ongoing alignment with CGA requirements, supported by the Legal and Technical teams.

13. Document Control & Updates

Version: 1.0

Effective Date: September 01, 2025

Last Reviewed: September 01, 2025

Next Scheduled Review: September 01, 2026

All updates must be logged and communicated internally. Material changes shall be reported to the CGA within the timelines prescribed by the National Ordinance.

14. Acknowledgement

This manual has been formally adopted by the Management of JarvisDelivery B.V. and is binding on all operational units and employees.