

Operational Manual

in accordance with Article 5.9 of the National Ordinance on Games of Chance (LOK)

Zeno Club B.V.

Incorporated in Curaçao under registration number: 154987

Contact: support@whiterabbit.casino

Version: 1.0

Effective date: September 1, 2025

1. Introduction

This Operational Manual (the “Manual”) is issued by Zeno Club B.V. (the “Company”) in accordance with the requirements of Article 5.9 of the National Ordinance on Games of Chance (the “LOK”) and forms an integral part of the governance system of the Company. Its purpose is to provide a detailed description of the operational structure, processes, systems, controls, and procedures through which Zeno Club B.V. ensures full compliance with the provisions of the LOK and with the conditions attached to the license issued by the Curaçao Gaming Authority. The Manual has binding force on all managers and employees of the Company and is subject to ongoing revision and improvement as the regulatory environment, business operations, the Company evolve but not less than once per quarter.

This Manual also functions as a compliance matrix against Articles 2.2(3), 5.3, 5.4, 5.6 and 5.9 of the LOK. Each operational control described below maps to one or more of these Articles and to the license conditions issued to the Company. Changes to this Manual follow a formal change control: the Compliance Officer maintains a version register, records the rationale, effective date, impacted systems and staff, and ensures acknowledgement by heads of department. Superseded versions are retained for five years. Emergency updates are permissible where necessary to remove an immediate risk to fair gaming, player protection or security, provided that a post-implementation review is completed within five business days and the permanent text is incorporated without delay.

The Company acknowledges that compliance with the LOK is not limited to technical requirements but also requires a culture of integrity, transparency, and accountability. Therefore, the Manual sets out not only technical standards but also policies of responsible gaming, fair play, protection of player funds and data, and proper handling of complaints and disputes.

2. Description of Games, Payments, Stakes, Payouts, Software and Outcome Determinants

The Company offers a wide range of gaming products to its players. These include slot games, table games such as roulette, blackjack, baccarat and poker, live dealer casino games streamed from certified studios, sports betting across pre-match and live events, and certain instant win and crash-type games. Each category of games is made available only after thorough due diligence on the provider, verification of the certification of the game software, and successful internal testing.

Game enablement follows a documented onboarding of each supplier and title, including verification of the game certificate, game math sheet, theoretical Return to Player (meaning percentage of prizes that will be returned to a player depending on funds deposited during the game initially; the “RTP”), payable version and build hash. A secure checksum registry is kept so that the binary or build identifier running in production can be matched to the certified artifact. Any change to RTP or critical parameters is treated as a material change and cannot be deployed

without re-certification or an explicit variance permitted by the certificate. For live casino, outcomes are generated by physical game play in certified studios; table layouts, shoe procedures, wheel maintenance and camera coverage are reviewed at onboarding, and the integrity of video streams is monitored to detect loss, delay or manipulation. For sportsbook, bet acceptance is rejected when the market is suspended or after event lock time; grading relies on official sources defined in the published settlement rules. Palpable error, late bets, abandoned or rescheduled events and dead-heat settlements are applied consistently with those rules and audit-logged to preserve the decision rationale.

The outcomes of the games are determined either by certified random number generators (the “RNG”), in the case of slots and table games, or by the actual play of physical games in the case of live dealer products, or by the official results of sporting events in the case of sportsbook operations. In all cases, the Company ensures that the method of determining results is transparent, auditable, and consistent with the rules disclosed to players.

Payments are accepted through various channels, including debit and credit cards, e-wallets, bank transfers, and where permitted by law, cryptocurrency solutions provided by regulated intermediaries. Deposits are credited immediately once authorized by the payment provider, and withdrawals are processed only after verification of the player’s identity and completion of AML checks. All fees, exchange rates and timelines are disclosed clearly to the player before the transaction is executed.

Player funds are credited upon provider authorization and are segregated in the ledger from operational funds. Withdrawal requests are queued for verification, including name-on-account matching, affordability and Responsible Gaming (the “RG”) checks, and AML screening. Where virtual assets are permitted, the Company uses risk-based blockchain analytics, screens originating and destination addresses, and withholds execution pending enhanced due diligence where red-flag indicators are present. Foreign exchange conversions display the applied rate and any fee before confirmation; the player must explicitly consent to the conversion. Negative balance creation is prevented except where explicitly allowed for settled adjustments.

The Company maintains strict controls on betting limits and payouts. Minimum and maximum stakes are set for each game and are published on the platform. The theoretical RTP percentages are monitored continuously, and actual payout data is reconciled with the theoretical expectations to detect anomalies. Progressive jackpots, if offered, are monitored in real time to ensure integrity and solvency.

3. Testing and Quality Control

The Company maintains a structured testing and quality control framework to ensure that all gaming products operate fairly and reliably. Prior to release, every game is tested by an independent accredited laboratory which certifies the randomness of the RNG, the accuracy of the payout percentages, and the conformity of the game mathematics with the disclosed parameters. Certificates are maintained in the Company’s compliance repository and are reviewed on a regular basis to ensure validity.

In addition to external testing, the Company conducts internal quality controls. All releases of software follow a strict change management process, which requires development, staging, and production environments to be separated. Every release is subject to a four-eyes principle, with approval required from both the technical and compliance teams. Automated monitoring tools supervise the games in production, and alerts are generated if abnormal payout patterns, technical

errors or suspicious activity is detected. Quarterly internal audits review active games, certificates, configurations, and payout reports.

4. Data Storage and Protection

The protection of personal and financial data of players is of paramount importance. All player data, including registration details, KYC documentation, transaction history and gaming activity, is stored securely in Tier IV certified data centers located in Curaçao. The data is encrypted both in transit and at rest. Access is restricted to authorized personnel only, through multi-factor authentication and role-based permissions. Logs of access and changes are maintained and reviewed regularly.

Data assets are classified as Public, Internal, Confidential and Restricted. Personal Identifiable Information (the “PII”), payment instruments, KYC files, game logs and financial records are restricted. Encryption at rest uses industry-accepted algorithms with keys protected by a centralized key management system; key rotation occurs at least annually or upon compromise. Access to Restricted data requires role authorization, multi-factor authentication and manager approval; quarterly recertification is performed and recorded. Backups are encrypted end-to-end and stored separately from production. The Company operates a Data Retention Schedule: core gaming and transaction records not less than five years; complaints files not less than five years from closure; access logs not less than two years; KYC documents not less than five years from the end of the relationship. Data subject requests are acknowledged within seven days and fulfilled within the statutory period following identity verification.

Data is retained for no less than five years in order to comply with legal obligations under AML/CFT regulations and to ensure availability for regulatory inspections. At the same time, the Company applies the principle of data minimization, ensuring that no unnecessary information is collected or stored. Players are informed about the processing of their data through a published Privacy Policy, and requests to exercise rights of access, rectification or erasure are processed in accordance with applicable law.

5. Visual Elements Presented to Players

The Company ensures that all visual elements displayed on its gaming platforms are clear, accurate and transparent. Players are provided with full access to the rules of each game, including bet types, payout odds, RTP percentages and maximum winnings. Account balances, transaction history, and applicable bonus terms are easily accessible from the player dashboard. Responsible gaming warnings and links to support services are displayed prominently. Reality checks and session timers are incorporated into the interface to remind players of the duration and extent of their play. The Terms and Conditions, Privacy Policy, and Complaints Procedure are accessible at all times. Tools for self-exclusion and cooling-off are available within the player account interface.

Reality check prompts appear by default every sixty minutes of continuous play and require a conscious action to continue. Limit changes that decrease exposure, such as lowering deposit or session limits, take effect immediately; increases take effect only after a twenty-four hour cooling-off period. The account area clearly shows verification status, any withdrawal holds with the precise reason, and a direct link to the Complaints Procedure and Alternative Dispute Resolution (the “ADR”) information. All promotional messages display the essential conditions up front, including wagering requirements and expiry, and never obscure material restrictions.

6. Access Restrictions for Prohibited Persons

The Company takes all necessary measures to ensure that persons who are not legally permitted to participate are excluded. Age verification processes are applied at registration, and proof of identity is required before the first withdrawal and, in certain cases, before play is permitted. Geolocation controls are used to block access from jurisdictions where online gaming is prohibited. The Company also maintains and consults self-exclusion and regulator-mandated exclusion lists. Accounts of such players are immediately blocked, and they cannot re-register.

Eligibility requires the player to be at least eighteen years of age or higher where mandatory locally. Identity is verified using government-issued photo ID and, where appropriate, biometric liveness checks. The Company maintains a unified exclusion registry across all brands and domains operated under its license; any self-exclusion request is actioned immediately and for no less than one year, and the account cannot be reopened before expiry. Geolocation is enforced at registration, login and payment, and the system denies connections from prohibited jurisdictions or sanctioned territories. Devices, IP ranges and payment instruments linked to excluded or under-age profiles are blocked to prevent re-registration.

Additionally, the Company screens all players against sanctions and politically exposed persons (the “PEP”) databases. Fraud detection systems using device fingerprinting and velocity checks monitor for attempts to create multiple accounts or to bypass restrictions. Continuous monitoring ensures that any breach is detected and addressed without delay.

7. Technical Infrastructure and Recovery

The Company’s technical infrastructure is designed to ensure security, stability and resilience. This infrastructure includes redundant load-balanced web servers, application servers, and database clusters with replication. Segregated environments are maintained for development, staging and production. Sensitive information and credentials are stored securely using encryption and key management systems.

Business Continuity prioritizes authentication, wallet, game session control, payment processing, KYC verification and customer support. The Recovery Point Objective is fifteen minutes and the Recovery Time Objective is four hours for these services. Backups are tested by quarterly full-restore drills, with evidence retained. Incident response operates a 24x7 on-call rotation, severity classification and communication plan; security incidents that may impact fairness, funds or PII are contained immediately, forensically preserved and notified to the regulator and affected players in accordance with legal timelines. A root-cause analysis is produced for every Severity 1 or 2 incident and tracked to closure.

8. Responsible Gaming

The Company implements Responsible Gaming measures pursuant to Articles 2.2(3), 5.4 and 5.6 of the LOK. Players can set deposit, loss, wager and session limits, and may activate temporary time-outs or self-exclusion; a self-exclusion remains valid for a minimum of one year. Monitoring uses behavioral markers of harm such as rapid deposit-loss cycles, escalation in stake size, multiple payment method failures and extended continuous sessions. Interventions follow a graduated model.

Level 1 involves contextual messaging and suggestions to set limits when early risk signals appear. Level 2 requires a proactive contact by trained customer support, an offer to apply limits or a cooling-off period, and a temporary freeze on promotions. Level 3 applies where harm indicators persist or accelerate and requires mandatory limits or a time-out imposed by the Company; withdrawals are still permitted subject to AML checks, but play is blocked. Level 4 is reserved for

acute risk or expressed distress and results in immediate suspension and assistance signposting; any reopening after suspension requires a cooling-off period and a formal review by Compliance.

Staff receive initial and annual training, including guidance on tone and escalation criteria, and all RG interactions are recorded and reviewed.

9. General Terms and Conditions

The General Terms and Conditions are maintained in a current version and are accessible at all times on the Company's website. They identify the licensee and the applicable law, set out account rules, eligibility criteria, KYC requirements, and define rules of play, bonus conditions, and expiry periods. They describe the procedures for deposits and withdrawals, including timelines, fees and currency conversion rules. They also include the full complaints and dispute resolution procedure, outline the responsible gaming commitments of the Company, and define prohibited conduct such as fraud, collusion or chargebacks. The Terms and Conditions are versioned and dated, and any changes are notified to players in advance.

The Terms and Conditions are governed by a formal lifecycle. Drafts are reviewed by Legal and Compliance, validated for clarity and fairness, and only then published with a version date and hash that is stored in the document register. Material changes are notified to players in advance, with the effective date clearly stated and updated on the Company's website; acceptance is recorded through a click-wrap mechanism. No clause may exclude a statutory right that applies under local consumer law. Where discrepancies exist between a promotion and the Terms and Conditions, the interpretation most favorable to the player is applied.

10. Dispute Resolution

Complaints may be submitted via email to support@whiterabbit.casino, via live chat or through the web form. Upon receipt, the Company issues an acknowledgement within forty-eight hours containing a unique case number, summary of the issue as understood, and the evidence requested. A Tier 1 handler conducts fact finding and aims to resolve the complaint within fourteen days. If unresolved or if requested by the player, the case escalates to Tier 2, where a senior reviewer reassesses the evidence and may request additional information; a final response is issued within twenty-eight days of the original receipt unless complexity justifies a longer period, in which case interim updates are provided at least weekly. The final response letter sets out the investigation steps, the decision with reasons, the remedy if any, and clear instructions for ADR escalation. Complaint files, including transcripts, evidence and decision logs, are retained for no less than five years. Unfair treatment or retaliation against complainants is prohibited.

If the player remains dissatisfied, the Company signposts an independent ADR entity recognized by the regulator. ADR outcomes are binding on the Company. Twice per year, the Company reports complaint volumes, categories, average resolution time and ADR referrals to the regulator and uses these metrics to improve processes.

11. Digital Records

The Company maintains complete, secure and tamper-evident records of all aspects of its operations. These include player identity and verification documents, account history, game session and round data, deposits, withdrawals, bonuses, adjustments, complaint files, ADR outcomes, and system access logs. All records are stored in Tier IV certified data centers located in Curaçao, with redundancy and backups. Records are retained for a minimum of five years and are accessible to the regulator at any time through secure interfaces.

Records include player identity data and verification artifacts; account lifecycle events; game session and round logs with timestamps synchronized to a trusted time source; deposits, withdrawals, bonuses, chargebacks and adjustments; complaints, RG interactions and ADR results; administrative actions such as limit changes and access rights modifications. Integrity is ensured through append-only storage for critical audit streams and cryptographic hashing to detect tampering. System clocks are synchronized with redundant network time protocols (the “NTP”) sources to prevent drift that could affect sequencing or fairness analyses. Exports to the regulator are provided through secure interfaces upon request.

12. AML/CFT Compliance

The AML/CFT framework forms part of day-to-day operations. Customer due diligence is completed prior to withdrawals and earlier where risk triggers exist, including high deposit velocity, multiple payment instruments, crypto usage, cross-border activity or adverse media.

The Company applies a risk-based approach with three levels of due diligence. Standard due diligence verifies identity and residence and screens for sanctions and PEP. Enhanced due diligence applies where the customer is high-risk or triggers thresholds and may require source of funds or source of wealth evidence, such as payslips, bank statements or proof of business income. Simplified due diligence may be applied only where justified by a demonstrably low risk and never contradicts statutory minimums.

Transactions and gameplay are monitored in real time against typologies such as structuring deposits and withdrawals, rapid churn, use of multiple accounts, third-party payments and unusual win-loss patterns.

Alerts are triaged by Risk and escalated to the Compliance Officer where suspicion is formed; the Compliance Officer documents the decision to report or not report and keeps a complete audit trail. All AML records, including alerts, investigations and reports, are retained in accordance with legal requirements. Staff performing onboarding, payments and risk monitoring receive initial AML training and annual refreshers.

13. Information Security and Business Continuity

Information security follows secure development and operations practices. Code changes undergo peer review and automated static analysis; dependencies are scanned for known vulnerabilities. Vulnerability management sets service level targets: critical issues are remediated or mitigated within twenty-four hours, high within seven days, medium within thirty days and low within ninety days. Penetration testing is conducted at least annually and after material changes.

Third-party suppliers undergo security due diligence, including review of certifications, breach history and incident obligations; contracts include security and audit clauses. Access rights are provisioned based on least privilege, reviewed quarterly and promptly revoked upon exit.

The Business Continuity Plan covers potential scenarios including loss of data center, cyberattacks, and supplier failures. Critical functions are restored within defined timeframes through redundant systems and tested disaster recovery procedures.

14. Transparency to Players

The Company is committed to transparency. Its identity, license details, and contact information are published on every page footer of its websites. Terms and Conditions, Privacy Policy, Responsible Gaming Policy, Complaints Procedure as well as other legal documents are easily accessible and always available in their most current version by the links:

- <https://www.whiterabbit.casino/en/help/50719/general-terms-and-conditions>
- <https://www.whiterabbit.casino/en/help/369727/player-account-fund-management-policy>
- <https://www.whiterabbit.casino/en/help/50720/privacy-policy>
- <https://www.whiterabbit.casino/en/help/95210/amlkyc-policy>

A dedicated status page informs players about scheduled maintenance or outages.

Marketing communications are truthful, do not target minors or vulnerable persons, and never misrepresent chances of winning. Bonus offers present material terms upfront. Affiliates must sign binding agreements requiring compliance with this Manual and applicable law; they are monitored and can be suspended or terminated for non-compliance. The Company prohibits any marketing during a self-exclusion or cooling-off period and honors unsubscribe requests without delay.

15. Training and Awareness

All employees undergo induction training covering regulatory obligations, responsible gaming, AML/CFT, and data protection. Refresher training is provided annually, and training is tailored for specific functions such as customer support, payments, or IT security. Training records are maintained for at least five years.

The curriculum covers LOK obligations, RG procedures, AML/CFT, data protection and security hygiene, with role-specific modules for customer support, risk and engineering. Staff complete an assessment after induction and annually thereafter; failure to achieve the passing score results in targeted retraining and re-assessment. Training completion and scores are recorded and retained for five years.

16. Internal Audit and Continuous Improvement

The Company operates an internal audit plan that periodically reviews compliance with this Manual. The internal audit plan is risk-based and covers at least once per year the following domains: game fairness and certification governance, payments and player funds reconciliation, AML/CFT controls, responsible gaming interventions, complaints and ADR handling, information security and access control, and data retention and exports.

Findings are graded by severity, corrective actions have owners and deadlines, and progress is reported monthly to senior management. Repeated or systemic issues trigger a thematic review. Root causes of any failures are identified and addressed. Quarterly review meetings are held with key stakeholders to review the Manual and approve necessary updates.

17. Document Control

This Manual is effective upon signature by the Compliance Officer and remains in force until replaced by a new version. The Compliance Officer ensures that the most recent approved version is accessible to staff at all times. Older versions are archived for inspection. Department heads attest annually that their teams operate in accordance with this Manual.

Each head of department provides an annual attestation that their procedures and controls are consistent with this Manual and with the license conditions, supported by evidence samples. The Compliance Officer compiles these attestations into an annual compliance statement retained for audit.

September 1, 2025

Compliance Officer

Lina Rače


