

Riotech N.V.

Operational Manual

Key Information

Policy Owner		Riotech N. V.
Approver		Boy Hendriks on behalf of statutory Director Ecorpp Management N.V.
Date approved		20 June 2026
Date last reviewed		20 June 2026
Review frequency		Annual
Next review date		June 2027
Responsible for document management		Derek Hendriks, Compliance officer
Security classification		Private and Confidential



Table of Contents

1. Purpose
 2. Operator Profile and Scope of Manual
 3. Description of the Games Offered
 4. Quality Monitoring and Testing Procedures
 5. Description of Visual Elements Displayed to Players
 6. Measures to Prevent Access by Prohibited Persons
 7. Technical Infrastructure and Business Continuity
 8. Responsible Gaming Measures
 9. Terms and Conditions
 10. Dispute Resolution Procedures
 11. Record Keeping and Data Retention
- Appendix A



1. Document Control and Source Hierarchy

1.1 Purpose

This Manual describes how Riotech N.V. operates its remote games of chance and how the operation complies with applicable Curaçao requirements and the attached internal operating documents. It is intended to be maintained as the Operator's operational manual for inspection by the CGA within the timeframe required by applicable law.

1.2 Review, update and availability

The Manual shall be reviewed at least annually and whenever there is a regulatory change, material operational change, change to licensed domains, change to software or critical suppliers, change to the Terms and Conditions, serious incident, or CGA request. Each review shall document the date, reviewer, scope of changes, and whether any amendment report or updated Manual must be submitted to the CGA.

1.3 Operational principles

Riotech N.V. operates its games of chance on the basis that the games must be safe, responsible, transparent, verifiable and reliable. The operational procedures in this Manual must be applied in a manner that supports player safety, fair and clear games, prevention of access by Vulnerable Persons, and player ability to limit or discontinue gambling where such gambling threatens to become harmful.

2. Operator Profile and Scope of Manual

2.1 Operator identification

Item	Details
Legal name	Riotech N.V.
Registration number	135400
Registered address	Heelsumstraat 51 E-Commerce Park, Curaçao.
Website	riobet.com
License number	OGL/2024/552/0560

2.2 Scope of the Manual

This Manual applies to all remote games of chance offered by Riotech N.V. through the domains and software applications listed by the Operator for the relevant Curaçao license. It covers operational procedures relating to game offering, player registration, player verification, payment handling, player protection, complaints, technical infrastructure, security, incident handling, reporting and record-keeping.

3. Description of the Games Offered

3.1 Product scope and game categories

The operator provides remote games of chance as defined under the LOK. The platform offers a variety of casino games including slots, table games, Live Casino, and other entertainment



options. The exact catalogue and number of games are provided by third-party game providers and may change.

3.2 Software providers and critical suppliers

The casino platform integrates games from multiple licensed third-party software providers (slots, live dealer games, etc.). Riobet acts as the operator providing access to these games under its Curaçao license.

The attached Terms and Conditions identify provider-specific restrictions for NetEnt games, NetEnt branded games and Microgaming games.

3.3 Outcome determination mechanisms

Game results are determined by a random number generator. For products whose results are not determined by the same RNG mechanism, such as fixed odds betting, live dealer products, poker or tournaments if offered, the relevant rules and settlement mechanisms must be completed by the Operator and aligned with the applicable game rules.

3.4 Game Rules, RTP, and Wagering Contribution

Detailed rules for each individual game can be found in the INFORMATION section on the main site.

- Go to the INFORMATION section.
- Click on Games Rules.
- Select the specific game to view its complete rules.

Inside the game rules players can familiarize themselves with the following information before playing on real money:

- RTP % — Return to Player (also called slot payout rate or theoretical return percentage). This shows the long-term theoretical percentage of wagered money that the game is designed to return to players.
- Wagering % — The contribution of bets placed in this game toward bonus wagering requirements (how much each bet counts toward fulfilling the wagering conditions of a bonus)..

3.5 Payment methods

Deposits and withdrawals are processed through the payment methods available in the Cashier section in accordance with Riobet's AML/CFT-compliant process. Both fiat and cryptocurrency options are supported.

Specific lists of supported methods, minimum/maximum amounts, and processing times are displayed in the account's Cashier and in the "Depositing and Withdrawing Winnings" Help Center



articles. The casino does not cover fees charged by payment providers. Repeated withdrawal requests may be subject to additional checks.

3.6 Betting, deposit and withdrawal limits

The attached Terms and Conditions set a minimum deposit and maximum daily deposit. They also provide player-level withdrawal limits in Appendix 3 and state that the daily maximum withdrawal may depend on the player's status. The bonus rules impose specific maximum bets and maximum bonus payouts while a bonus is active.

3.7 Payout mechanisms

Players may request withdrawals provided deposits have cleared, required verification has been completed and AML/CFT checks do not prevent payment. The withdrawals must generally be made through the same payment method and details used for deposit, subject to the Operator's AML/CFT policy.

Withdrawal limits applicable to a player's account are determined by player status and payment method as set out in the Deposits and Withdrawals schedule in Appendix 3 of the Terms and Conditions. Where any general withdrawal limit stated elsewhere in the Terms and Conditions conflicts with the status-based limits in Appendix 3, the Appendix 3 schedule shall prevail as the operative limit schedule. The Operator shall ensure that the player-facing account area reflects the applicable status-based limits at all times.

3.8 Prohibited game content and credit prohibition

The Operator shall not offer games whose outcome depends on disasters, crises, exploitation or abuse of human beings or animals, or other events jeopardising life, and shall not offer offensive or dishonourable games. The Operator shall not provide players with any form of credit and shall not act as an intermediary in providing credit.

4. Quality Monitoring and Testing Procedures

4.1 Quality monitoring framework

Quality monitoring covers game fairness, system integrity, transaction integrity, security, responsible gaming controls, AML/CFT controls, complaints handling and supplier performance. Monitoring is performed through a combination of automated transaction and fraud monitoring, customer file reviews, security risk assessments, incident reporting, complaint logs, supplier reviews, backups, and periodic compliance reviews.

4.2 System monitoring

The Operator shall monitor system activity to identify security breaches, unusual player activity, potential fraud, misuse of games, AML/CFT concerns, problem gambling indicators, duplicate accounts, attempts to bypass limits, and system failures. Monitoring outputs shall be escalated to the responsible authorised person.



- Information security monitoring includes regular audits, monitoring systems to detect and respond to security breaches or suspicious activity, perimeter controls, antivirus/antimalware protection, firewalls, VPNs, encryption, intrusion detection and intrusion prevention systems.
- AML/CFT monitoring includes continuous transaction monitoring, alerts for unusual or inconsistent activity, review of deviations from customer profile and assessment of whether SAR reporting is required.
- Responsible gaming monitoring includes deposit activity, wagering patterns, session durations, player interactions, requests for bonuses, cancelled withdrawals, changes to limits and attempts to open multiple accounts.
- Complaint monitoring includes maintenance of a secure complaint log and bi-annual reporting of complaint volume, status, categories and outcomes to the CGA.

4.3 Testing procedures

The Operator shall maintain periodically used test methods for quality monitoring.

4.4 Incident management

Information security incidents must be reported to the Director. The Operator's management system is used to manage system changes and provides details about the timing, authorship, nature and progression of each alteration. The Director has primary oversight and accountability for incident management under the Information Security Policy. Staff and authorized users who become aware of an information security incident must report it to the Director.

For CGA reporting, incident reports must be filed within 24 hours of an incident where the event falls within the reporting categories set out by the LOK, including gaming security breaches affecting personal information or game details, equipment/software failure or damage causing loss of all or part of remote games, gaming-related attempted fraud or criminal behavior, or other events threatening responsible, reliable and verifiable game organization or public trust.

4.5 Compliance reviews

Compliance review procedures shall include: annual review of internal policies; review of the risk appetite annually or upon significant business change; monthly identification of customer files due for periodic review; monthly dormant account checks; bi-annual complaint reporting; annual responsible gaming and information security document reviews; and periodic independent AML/CTF audit. Findings shall be documented, assigned to owners and tracked to remediation.

5. Description of Visual Elements Displayed to Players

5.1 Before registration

Before or during registration, the player-facing interface shall present or make available the information required by the Terms and Conditions and CGA T&C guidance. The current version of the Terms and Conditions must be available in a clear and readable form, accessible within one click from the homepage, registration page and player account area. During registration, the player must actively acknowledge:

- acceptance of the Terms and Conditions, Licensee identity and regulatory status, including legal name, registered address, registration number and current CGA license details.



- Age eligibility and minimum legal age statement, including that underage players may not use the services.
- Jurisdictional restrictions and player responsibility for lawful participation.
- Privacy Policy, AML/KYC information and Responsible Gaming information.

5.2 During gameplay and account use

During gameplay and account use, the platform shall make available information required to support transparency, responsible play and player account control. The source documents support display of account balance, transaction history, betting/wagering history, session timing/reality check information, responsible gaming tools, game rules, bonus terms and crypto exchange information where applicable.

- Transaction history is available through the “Finances” link according to the attached Terms and Conditions.
- Players shall have access to a detailed record of their betting and wagering history, including timestamps of transactions from account opening.
- A real-time session timer shall remain visible while the player is logged in, and player-activated reality checks may be set at specified intervals.
- Responsible gaming tools, including deposit limits, time-outs/cooling-off and self-exclusion, shall be clearly presented in the player account interface.
- Where Bitcoin is offered, the Bitcoin to fiat exchange rate shall be displayed on the homepage and volatility information shall be provided.

5.3 Mandatory notices and disclosures

Disclosure	Operational requirement
Terms and Conditions	Current T&C accessible within one click; changes notified; material changes require active re-acceptance.
Licensee information	Legal name, registered address, registration number, CGA license number, license issue date and licensee name.
Jurisdiction and age	Minimum legal age, prohibited territories and player responsibility.
Responsible gaming	Self-exclusion, cooling-off, limits, signs of problem gambling and external support links.
Complaints	Complaint channels, timelines, CGA non-mediatory



	role and CGA regulatory complaint link.
Bonuses	Wagering requirements, bonus expiry, forfeiture, withdrawal restrictions and maximum bonus-related bets/payouts.
Fairness and game rules	RNG result statement and discrepancy resolution through server records; game rules and any non-RNG settlement rules.

6. Measures to Prevent Access by Prohibited Persons

6.1 Prohibited and restricted persons

The Operator shall not give access to underage persons or any person who must within reason be assumed to be a Vulnerable Person. Under the LOK, Vulnerable Persons include persons under eighteen, persons unable or insufficiently able to control gambling behaviour, persons banned from games of chance voluntarily or compulsorily, and persons declared bankrupt or otherwise lacking control over their property. A player must also not play a game where they already know the outcome of the relevant event or where they qualify as a Key Person of the provider.

6.2 Age verification procedures

Age control starts at registration. New players must provide identity and age-related registration information. Customers under the legal gambling age are strictly prohibited.

6.3 Jurisdictional restrictions

The Operator shall apply jurisdictional restrictions stated in the current Terms and Conditions and provider-specific territorial restrictions for particular game providers. The Operator shall ensure that restricted territories are reflected in registration controls, payment processing and game availability controls.

6.4 Self-excluded and restricted players

Self-exclusion is implemented immediately and applies across all domains, brands and platforms operated under the same license and customer account. Self-exclusion requests must be irreversible during the selected duration. Internal and third-party self-exclusion lists are used to prevent duplicate registrations or reactivation attempts under different identities. If a customer's name appears on a self-exclusion list during onboarding or screening, the customer's account cannot be opened.

6.5 Account monitoring controls

The Operator monitors account activity to identify duplicate accounts, fraud, use of bots, exploitation of software errors, money laundering, criminal activity, collusion, suspicious deposits and withdrawals, attempts to bypass limits, use of multiple payment methods, and responsible gaming concerns. One account is permitted per player, household, IP address, postal address, computer or device. Suspicious or prohibited activity may result in investigation, account suspension, account



closure, voiding of transactions, cancellation of winnings or reporting to the relevant authorities, subject to the applicable Terms and Conditions and AML/CFT procedures.

7. Technical Infrastructure and Business Continuity

7.1 Technical architecture overview

Riobet operates as a modern, scalable online casino platform designed for high availability, security, and seamless integration with multiple third-party providers. The architecture follows a typical multi-tier, microservices-oriented design, optimized for performance, regulatory compliance, and global player access.

Core Components

Frontend Layer (Client-Side)

- Responsive web application built with modern frameworks ensuring compatibility across desktop, tablet, and mobile devices.
- Instant-play (no-download) games via browser.
- Fast loading for static assets, images, and game clients.
- User interface includes account management, cashier, game lobby, and live casino streaming.

Backend Layer (Application & Business Logic)

- API-driven architecture with secure endpoints for real-time features (e.g., live betting, balance updates).
- Player Account Management (PAM) system handling registration, authentication, KYC verification, session management, and responsible gaming tools.
- Wallet and transaction engine for real-time balance updates, bonus management, and wagering calculations.
- Game integration layer (aggregator) that communicates with third-party game providers via secure APIs.

Game Integration & Providers

- Seamless integration with licensed game suppliers
- RNG Games: Server-side calls to certified Random Number Generators hosted by providers. All outcomes are fully independent and audited.
- Live Casino: Low-latency video streaming integration with dedicated studios. Real-time synchronization between dealer actions and player bets.
- Demo mode support.

Payment & Financial System



- Integrated payment gateway supporting multiple fiat and cryptocurrency methods.
- Secure processing with tokenization and encryption.
- Automated deposit/withdrawal workflows with compliance checks (AML, fraud detection).
- Multi-currency wallet support.

Database & Storage

- Robust, ACID-compliant databases for player data, transaction history, game logs, and financial records.
- Caching layers for high-speed session and balance operations.
- Secure audit logging for all player actions and system events to ensure regulatory compliance.

Security & Compliance Layer

- Industry-standard encryption for all data in transit.
- Advanced DDoS protection, WAF (Web Application Firewall), and anti-fraud systems.
- Full account verification (KYC) module.
- Compliance with Curaçao Gaming Control Board requirements, including data protection, fair gaming, and anti-money laundering policies.
- Provably fair mechanisms where applicable and certified RNG audits by independent labs.

Infrastructure & Scalability

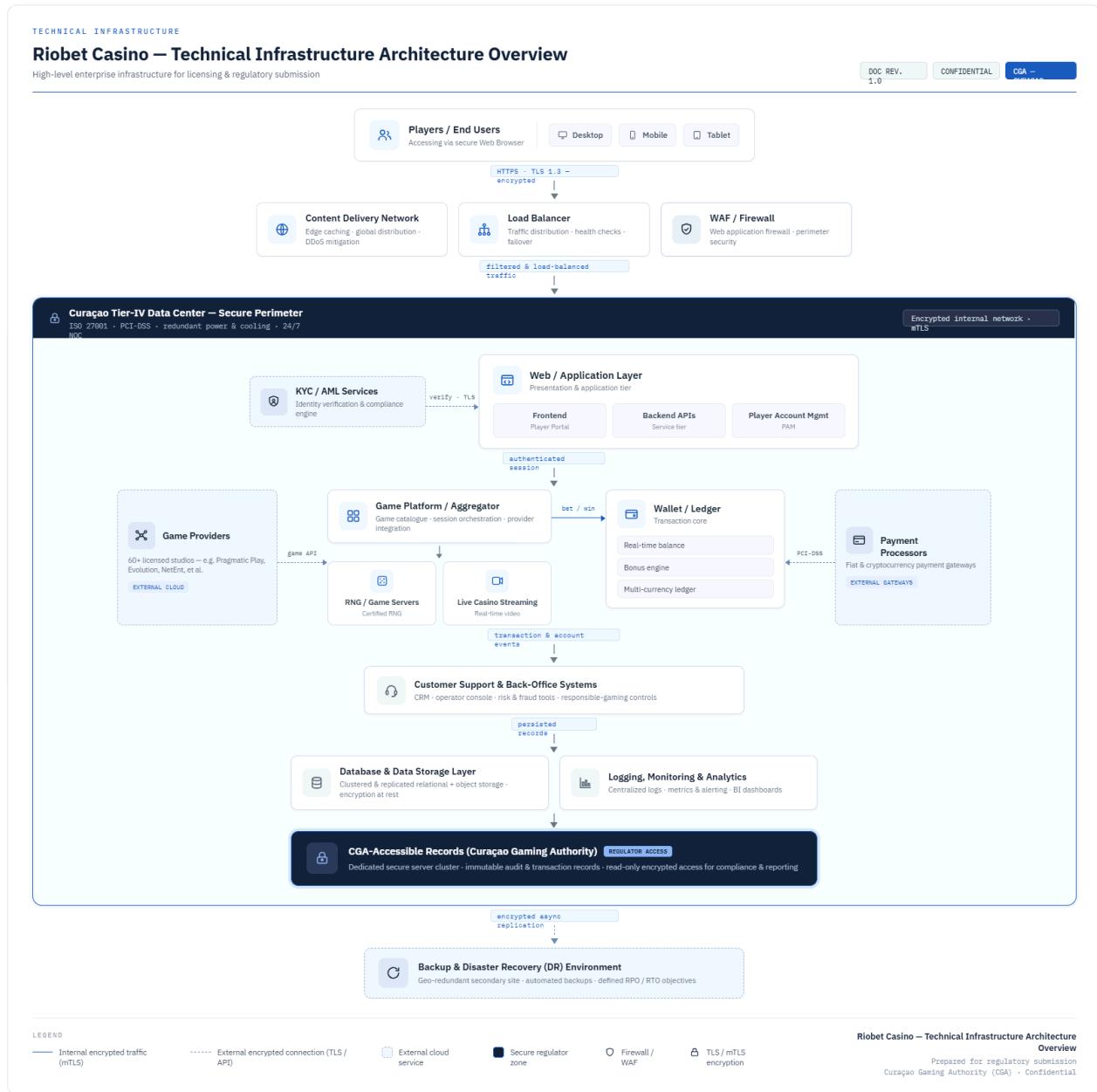
- Hosted on reliable, high-availability cloud or dedicated infrastructure with redundancy and failover capabilities.
- Horizontal scaling to handle peak concurrent users.
- Monitoring, logging, and alerting systems for 24/7 operational stability.
- Multi-language and multi-currency support for international audiences.

Administration & Back-Office

- Operator dashboard for managing bonuses, promotions, player support, reporting, and analytics.
- Real-time monitoring of game performance, payouts, and system health.



7.2 Infrastructure diagram



7.3 Hosting arrangements

Digital records of critical information about players, gaming transactions and financial transactions are kept by the Operator available to the CGA at all times on a server of a Tier-IV certified data center registered in Curaçao.

7.4 Data security measures

The Operator applies information security measures designed to protect confidentiality, integrity and availability of information. Access to Company information, resources, services and physical premises is restricted and controlled on a need-to-know basis. Access rights are assigned, audited and removed

through an access control process. Users and third parties must have appropriate confidentiality and data protection provisions before access is granted.

7.5 Disaster recovery procedures

Server systems undergo regular backups using a standardized methodology. Backup media is transferred and securely stored on-site or off-site. Sensitive and confidential Company information is encrypted during backup and capable of authorized decryption for the legally or regulatorily required period. Backup systems are periodically tested to verify that procedures function as intended.

7.6 Business continuity arrangements

Riotech N.V. maintains a business continuity plan that assigns defined roles and responsibilities to designated Key Persons and operational leads for the management of service interruptions, technical emergencies, cyber incidents, and supplier failures. Recovery priorities are determined by the criticality of the affected service to player safety, transaction integrity, and regulatory reporting capability, with player account access, payment processing, and CGA-accessible records treated as the highest-priority restoration targets. Recovery time and recovery point objectives are defined for each critical system and are reviewed annually and following any material incident or infrastructure change. In the event of a service interruption, a structured communication plan governs internal escalation to the Director and relevant operational owners, player-facing notifications where required, and, where the interruption constitutes a reportable incident under LOK Article 5.10, submission of an incident report to the CGA through the CGA online portal without delay.

8. Responsible Gaming Measures

8.1 Player protection controls

Responsible gaming controls are designed to keep gambling as entertainment and to reduce the risk of gambling-related harm. The Operator provides information about responsible gambling tools, problem gambling signs and support resources on the homepage, footer and Responsible Gaming Policy. Players can access betting and wagering records and may use self-assessment tools such as the Gamblers Anonymous 20-question quiz or an adapted CAGE questionnaire.

8.2 Cooling-off and self-exclusion

Players may activate short-term cooling-off periods through the account interface or customer support while technical solutions are being implemented. Available cooling-off durations are 24 hours, 7 days, 1 month and 3 months. Once requested, cooling-off is applied immediately and is irreversible for the selected duration. During cooling-off, the player is logged out, prevented from logging in, unable to deposit or wager, and marketing communications are suspended.

Self-exclusion options are 1 year, 3 years, 5 years, 10 years and indefinite lifetime exclusion. Self-exclusion is immediately enforced, applies across all domains, brands and platforms operated under the same license and customer account, and includes a ban on all marketing communications.

8.3 Deposit, wagering, loss and session limits

Players may set daily, weekly or monthly deposit limits through the account dashboard. Reductions in deposit limits take immediate effect. Increases in deposit limits are subject to a mandatory seven-



day cooling-off period before taking effect. Depending on target market and player demographics, players may also be provided with loss limits, session time limits and wagering limits. All limits and changes shall be logged, timestamped and enforced through automated system controls with compliance and support oversight.

8.4 Detection of problematic gambling behaviour

The Operator monitors for indicators of problematic gambling behaviour, including sudden increases or erratic deposit/wagering/session patterns, use of multiple payment methods to bypass limits, repeated cancellation of withdrawals, extended sessions without breaks, increased customer support contact, requests for bonuses, agitation, frequent changes to responsible gaming tools, young players spending substantial amounts, maxing out cards and attempting to register additional cards, unrealistic spending patterns and attempts to open multiple accounts.

When concerning behaviour is identified, direct player contact is initiated, interactions are documented in the player account management system, the player is informed about responsible gaming tools, and proportionate interventions may be applied, including deposit limits, temporary suspension pending review, or exclusion in extreme risk cases. Problematic behaviour is escalated to the Compliance Officer, who assesses account history, previous interventions and risk level.

8.5 Responsible gaming communications and support

All responsible gaming communications produced or published by Riotech N.V. shall be clear, accessible, factually accurate and directed toward player protection. Communications shall not minimise the risks associated with gambling or be presented in a manner that could discourage a player from making use of available protective tools.

Players shall be directed to both internal responsible gaming tools and to external support organisations.

Links to responsible gaming support resources shall be maintained and kept current on the Responsible Gaming page, the homepage, the login-area footer, all safer gambling communications, account limitation notifications and throughout the self-exclusion process. Riotech N.V. shall review the accuracy and availability of all external support links as part of its annual responsible gaming policy review.

8.6 Responsible marketing

All marketing and advertising conducted by or on behalf of Riotech N.V., including bonus and promotional communications, shall comply with the responsible marketing requirements of the LOK and the Riotech N.V. Responsible Gaming Policy.

Marketing communications shall not encourage excessive or uncontrolled gambling, shall not be misleading as to the nature, odds or potential outcomes of games, and shall not be directed at or



designed to appeal to Vulnerable Persons, including persons who are underage, self-excluded, subject to cooling-off, or otherwise identified as at risk. Direct marketing shall be suspended immediately upon activation of a cooling-off period or self-exclusion and shall not resume until the relevant period has expired and the player has not renewed or extended their exclusion.

Promotional messaging shall not portray gambling as a solution to financial difficulty, a source of income, or a means of achieving personal or social success. Marketing materials shall not employ aggressive or deceptive tactics, imagery designed to appeal to persons under eighteen, influencers whose primary audience is under eighteen, the appearance or likeness of minors, sexually explicit content, or any association with conduct or behaviours that are harmful or unlawful.

Riotech N.V. shall maintain a marketing approval process under which all new promotional content is reviewed for compliance with this policy before publication. Affiliate marketing arrangements shall be subject to equivalent standards, and compliance with responsible marketing obligations shall be included in affiliate agreements and monitored on a periodic basis.

8.7 Minor or self-excluded player access incident procedure

If a self-excluded individual or minor is found to have accessed gambling beyond their exclusion choices or age restriction, Riotech N.V. must immediately block the account, refund all deposited amounts except funds frozen in accordance with AML policy within two business days, and submit a detailed report to the CGA within five working days explaining how the issue occurred and what actions are being taken to prevent recurrence.

9. Terms and Conditions

9.1 Current Terms and Conditions status

The attached player-facing Terms and Conditions in the Appendix A are treated as the current operational source document for riobet.com.

10. Dispute Resolution Procedures

10.1 Complaint submission process

Players may submit a complaint in relation to any aspect of the services provided by Riotech N.V. free of charge and within six months of the date of the relevant event or, in the case of an ongoing game or event, within six months of the final resolution of that event. Complaints must be submitted in writing using the official complaint submission form available on the Website or by email to support@riobet.com. The complaint submission must include the player's full name, account number, date of the relevant event, a description of the issue and any supporting documentation the player wishes to rely upon.

10.2 Internal Review and Resolution Timelines



Upon receipt of a complaint, Riotech N.V. shall acknowledge receipt in writing as soon as practicable. Where a shorter acknowledgement timeline is published in the player-facing Complaints Policy or on the Website, that timeline shall apply. In all cases acknowledgement shall be provided no later than seven calendar days from receipt of the complaint, setting out a summary of the complaint as understood, the applicable resolution process and the estimated resolution timeline. Complaints relating to responsible gaming, including self-exclusion breaches and protection of Vulnerable Persons, shall be treated as a priority and resolved within five business days of receipt. All other complaints shall be resolved within four weeks of receipt. Where the complexity of a complaint or the need to obtain further information requires additional time, the resolution period may be extended once by a further four weeks, provided that the player is notified of the extension and the reason for it before the original deadline expires. All determinations shall be provided to the player in writing and shall be reasoned.

10.3 Escalation to Alternative Dispute Resolution

Where a complaint has not been resolved through the internal process within the applicable timeframe, or where the player is not satisfied with the outcome of the internal process, the player is entitled to refer the dispute to an independent Alternative Dispute Resolution provider certified by the CGA. ADR is available to players free of charge; Riotech N.V. shall bear all costs of the ADR process.

10.4 Notification of Regulatory Breach — Curaçao Gaming Authority

The CGA does not mediate individual disputes between players and operators. Where a player considers that Riotech N.V. is acting in breach of its license conditions or applicable Curaçao law, the player may notify the CGA directly by submitting a report through the official CGA regulatory complaints channel at complaints@cga.cw. The CGA will use information submitted to it for the purpose of supervisory oversight and monitoring of operator compliance; it will not intervene as a party to an individual player dispute. The existence of this channel shall be disclosed in the player-facing Terms and Conditions and the public-facing Complaints Policy of Riotech N.V.

11. Record Keeping and Data Retention

11.1 Record-keeping principles

Records are maintained so that the Operator's rights and obligations and the player's rights are clear at all times, and so the Operator can respond within a reasonable period to CGA requests for data required to supervise compliance. Access is restricted on a need-to-know basis and according to information classification.



11.2 Player records

Player records shall include registration details, acceptance of Terms and Conditions and Privacy Policy, marketing consent status where provided, identification and verification documentation, age verification attempts and outcomes, CDD/EDD records, risk ratings, PEP and sanctions screening results, source of funds/source of wealth information where requested, safer gambling questionnaire responses where applicable, account status, account restrictions, self-exclusion and cooling-off records, player communications and support interactions.

11.3 Gaming transaction records

Gaming transaction records shall include bets, wagers, game results, game rules applied, server records of game outcomes and account balances, transaction timestamps, wagering history, bonus wagering progress, tournament/game participation and any discrepancies between player device displays and server records. The player must be able to view transaction history via the relevant account interface as stated in the Terms and Conditions.

11.4 Financial transaction records

Financial transaction records shall include deposits, withdrawals, payment methods, payment instrument identifiers where applicable, crypto wallet information where applicable, deposit and withdrawal amounts, cleared payment status, chargebacks/reversals, source-of-funds/source-of-wealth records where requested, AML alerts, transaction monitoring reviews and SAR-related internal records. Gambler transaction reports to the CGA must include the total amount, nature of the crediting and debiting of a gaming account, nature of payment instrument used where applicable, and a unique identifier not directly traceable to the player's identity for each payment account debited or credited for each registered domain or software application.

11.5 Retention periods

Record type	Retention period / rule
AML/KYC and customer relationship records	Five years from the date the customer relationship ended, unless longer retention is required by law, regulatory review/investigation, legal proceedings or justified consent.
Complaint records	Five years.
Terms and Conditions archive and acceptance evidence	Historical archive from the first uploaded Terms and Conditions; player acceptance/non-acceptance logs retained and available to CGA upon request.

Training records	Five years
Information security records and backups	No longer than required unless justified by legal, regulatory or business need; backup media archived according to retention requirements.

11.6 Storage and access controls

Records are stored securely according to information classification. Confidential and restricted records are accessible only to staff with a legitimate need and appropriate authorization. Remote access is controlled by Director-approved VPN and two-factor authentication. Confidential data in transit or cloud storage must be encrypted where required by the Information Security Policy. Backup media is securely stored and periodically tested for restore capability. The Operator must ensure that critical records required by the LOK remain available to the CGA at all times on a server of a Tier-IV certified data center registered in Curaçao.



Appendix A

TERMS AND CONDITIONS

A handwritten signature in black ink, consisting of stylized, overlapping loops and lines.