

ALISIUM B.V.

OPERATIONAL MANUAL

2026

Table of Contents

1. Version Control	3
2. Overview	4
3. Regulatory framework	4
4. Operational framework	4
5. Quality Monitoring	6
6. Data privacy	6
7. User Interface and Visual Presentation	9
8. Admission restrictions	10
9. Technical Infrastructure	10
10. Responsible Gaming Principles	12
11. Terms and Conditions	14
12. Dispute Resolution	15
13. Critical data storage	15



1. Version Control

Name	Description
Document Name	Operational Manual
Version	1.0
Owner/Responsible department	Compliance Department
Authorised By	Board of Directors
Latest Distribution and Effective Date	25.06.2026
Next Review Date	25.06.2027

Version	Description	Date	Initials
1.0	Policy implementation	25.06.2026	



2. Overview

Alisium B.V. (hereinafter “the Company”) is a limited liability company established under the laws of Curaçao, registered with the Chamber of Commerce of Curaçao under number 161507. The Company is a holder of the B2C license number OGL/2024/227/0112 to operate games of chance and is regulated and supervised by the Curacao Gaming Authority (CGA).

The Company has developed this operational manual containing information about the manner and degree of compliance with the provisions laid down in or under the NATIONAL ORDINANCE of the 20th of December 2024 containing Rules concerning Games of Chance (National Ordinance on Games of Chance), hereinafter “LOK” and the rules and restrictions attached to the Gaming License of the Company.

3. Regulatory framework

1. NATIONAL ORDINANCE of the 20th of December 2024 containing Rules concerning Games of Chance (National Ordinance on Games of Chance) - LOK¹
2. CGA issued regulatory policies and guidelines²
3. CGA defined license conditions and restrictions

4. Operational framework

Types of Games of chance offered by the Company are as follows:

1. Games of Chance (RNG-based games such as slots and casino table games)
2. Betting (including live betting and virtual-sports betting)
3. Live casino
4. Sports betting
5. Pooled-prize games
6. Poker

Games offered are channelled through PC/Desktop and are implemented from third-party game providers. All games are supplied exclusively by licensed third-party providers and are certified in accordance with applicable regulatory requirements, including RNG (Random Number Generator) certification and other required technical compliance standards, ensuring fairness and

¹ <https://portal.cga.cw/uploads/publications/sV4kfJ6psZ9WM80fMSimTq95RBLTuG5TJ1nuBhyp.pdf>

² <https://portal.cga.cw/articles>



integrity of game outcomes. The outcome-determining elements of all games are based on certified RNG systems provided by licensed game suppliers. Game results are generated automatically and cannot be influenced or controlled by the operator, ensuring fairness, randomness, and compliance with applicable gaming standards. The Company ensures that RNG certificates / test lab certifications are maintained at all times for all the games offered.

Bet amounts are defined per game and may include minimum and maximum limits as specified in the individual game rules, which are available to players prior to participation and at all times after. Specifically games rules are available on the main website page in the Games Rules Section. Players are able to review all applicable wagering conditions and rules directly on the website before engaging in the gaming activity.

Types of payment method offered by the Company are as follows:

1. Card payments
2. E-wallet payments
3. Wire transfers
4. Virtual currency payments
5. Other methods, which may be approved by the Company or respective regulators from time to time

All payment transactions are processed through licensed financial institutions and authorized payment service providers. Cash payments are not accepted under any circumstances. The Company also does not operate any land-based casino premises or affiliated land-based casino facilities.

The Company shall accept only those payment methods, which belong to the players and not to any other third party. The Company also follows the closed-loop payment rules, meaning the players are paid out to the same payment method from which deposits were received, where this is possible. Verification and AML rules apply before any payout can be processed, as specifically described in the Companies AML/CTF/CPF policy and Terms and Conditions available to the players on the website at all times. Payouts are processed in accordance with the Terms and Conditions available on the website at all times. Minimum and maximum withdrawal limits may apply, as specified in the T&C. In cases where withdrawal amounts exceed internal processing limits, payments may be executed in installments. The latest version of Terms and Conditions can be found in Annex 1 to this Operation Manual.



5. Quality Monitoring

To ensure the secure, reliable, and uninterrupted provision of its services, the Company conducts its operations through a platform that is duly certified in accordance with ISO 27001 standards. Regular audits, assessments, and testing procedures are performed to verify ongoing compliance with applicable ISO requirements and to ensure continuous monitoring of information security, service quality, and operational resilience.

In addition, all games supplied by third-party providers are subject to regular testing, certification, and verification in accordance with applicable regulatory requirements and recognized industry standards, ensuring the integrity, fairness, and reliability of gaming outcomes.

6. Data privacy

Players' personal data and other related information are stored in full compliance with applicable data protection laws and regulatory requirements.

All data is hosted on Tier IV-certified servers located in Curaçao, ensuring a high level of infrastructure reliability and security. Regular mandatory backups are performed to ensure data integrity and availability.

Types of Personal Information which is collected and stored:

1. identification information
2. financial information;
3. copies of identification documents
4. personally submitted preferences;
5. recordings of telephone conversations and website activity;
6. responses to competitions, other promotions, and surveys;
7. profession, occupation, or job title.

The above list is not exhaustive, and other types of information may be collected during business relationships with the player for proper compliance and cooperation purposes. However the data is always collected and stored only for the legal purpose, and the players are notified about the fact of data collection and storage through the Privacy policy always available on the website.

Personal information is being collected only by lawful and fair means.

It is collected directly from the player unless it is unreasonable or impracticable to do so. The following are instances of data collection:



- Account registration;
- Access or use of website or app (including cookies);
- Use of products and services;
- Participation in competitions, giveaways and other promotions;
- Contacting the Company directly via any medium including: SMS, MMS, instant messaging, email, social media platforms, postal mail and telephone;
- Feedback provision through the website/app feedback links;

For compliance purposes data may also be collected from the third parties, such as credit reporting agencies, law enforcement agencies, and other government entities; identity verification providers.

Legal basis for data collection, storage, use and disclosure

Personal data is collected, stored, used, and disclosed for the following purposes:

- to allow players to register as a client;
- to provide products and services to the players;
- to enable the Company to perform obligations to the players under the Terms of Use, and to ensure that the players perform obligations under the Terms of Use;
- for communicating with the players, including sending information about our products and services;
- for planning, research, promotion, and marketing of the Company's goods and services, including conducting competitions or promotions;
- to create aggregate data about clients through demographic profiling and statistical analysis of the Company's database to optimise our products and services and /or allow for more efficient operation of the business;
- to maintain a credit information file on players and to carry out a credit assessment on players;
- to establish player bona fides;
- for the investigation of suspected unlawful, fraudulent, or other improper activity connected with the use of the Company's products and services; and
- to comply with the legal and statutory obligations, including obligations relating to identity verification and reporting under the Anti-Money Laundering and Counter Terrorism Financing legislation and other applicable laws.

Personal Information Disclosure:

Personal information is shared with other entities in the Company's group in a strictly controlled manner and is not sold to other companies.



The Company may disclose players personal information to third parties as follows:

- to a credit reporting agency;
- to the Company's contractors and external service providers associated with the operation of the business and provision of the services including, without limitation, associated data centres, web hosting providers, payment service providers, identification verification service providers, advertising agencies, mailing houses, printers, call centres, market research analysts, IT consultants, professional advisors and consultants;
- to law enforcement agencies to assist in the prevention of criminal activities;
- to government and regulatory authorities and other organisations as required or authorised by law or otherwise;
- controlling bodies where such controlling bodies request information to protect and maintain the integrity of services provided or where we consider any betting or gaming activity to be suspicious or unusual; and
- to a successor entity in the event of a business transition, such as a merger, corporate reorganisation or to a purchaser of part of or all of the Company's assets.

Should the information be transferred to a third party, the Company shall use reasonable endeavours to ensure that the information disclosed is protected by the third party under contractual arrangements.

Data security

The Company takes reasonable steps to protect the collected personal information and ensure that it is accurate, complete, and up-to-date. The information is held on secure servers, such as TIER-IV certified Curacao servers. Personal information may also be stored in telephone recordings and in hard copy or paper files.

The employees, agents, contractors are required to maintain the confidentiality of all personal information.

The Company stores all of the Personal Information received directly from players in the protected database residing within the secure network behind active state-of-the-art firewall software. The Company's services support SSL Versions at least TLS 1.2, but mostly TLS 1.3 with 256-bit encryption. HTTP/2 and QUIC protocols are supported as well.

Overseas transfer of personal information

There may be instances where the Company may be required to send personal information overseas or collect personal information from overseas, including:



- where the players have asked the Company to do so;
- when the Company has outsourced a business activity or function to an overseas provider with whom it has a contractual arrangement; or
- where the Company is required or authorised by law to do so.

Personal information may be disclosed to entities located outside player's country of residence, including the following:

1. companies within the Company's group; and
2. external service providers.

Unsolicited personal information

Where the Company receives unsolicited personal information, it will be determined whether or not it would have been permissible to collect that personal information if it had been solicited. If it is determined that collection would not have been permissible, to the extent permitted by law, it will be destroyed or de-identified as soon as practicable.

The Company's Privacy Policy, which outlines in detail the principles and procedures for the storage and processing of players' personal data, is published on the website and is at all times accessible to players.

7. User Interface and Visual Presentation

The following minimum visual elements are always available to players through the gaming website:

- 1) Casino name and Registration details of the Company, incl. At least full name, reg. Number, reg. Address, licence number and supervisory authority
- 2) Validator
- 3) List of games
- 4) List of payment options available
- 5) Language switch
- 6) Registration Form
- 7) Age restriction icon (18+)
- 8) Policies and guidelines, incl.: Privacy Policy, Responsible Game, Fair play, Games Rules, Terms and conditions, Support Contact details, Complaints Procedure
- 9) Player profile information, including: Real and Bonus balance, Loyalty points and level, transaction, betting, bonus and tournament history, registration details, subscriptions switch, password change option, verification section, responsible gaming section with tools for self-setting limits, description about the responsible gaming functionality and link to self-assessment questionnaire
- 10) Search bar



- 11) Payment functionality, including deposit and withdrawal functionality
- 12) Complaint submission form
- 13) Promotions

8. Admission restrictions

The following technical and organizational measures are implemented by the Company to prevent access to the website or usage of offered products and services by the natural persons, who are banned under LOK provisions:

- 1) Age verification and confirmation at the registration point, not allowing registration for minor players
- 2) Verification and KYC procedures, allowing detect vulnerable persons or players from the restricted countries
- 3) Automatic technical restriction based on registration and each access IP address / geolocation of the player, not allowing access to the players from restricted areas
- 4) Sanctions screening program to detect and ban persons, subject to international sanctions regimes
- 5) Technical restriction to access the profile, if self-exclusion has been set (both self-set or forced, i.e. set by the Company based on the vulnerability assessment of the Company)
- 6) Any employee / officer / key persons of the Company - Verification and KYC procedures in place to ensure such accounts are blocked. Relevant provisions in the labor agreement.

These measures are supported by ongoing monitoring and compliance checks.

9. Technical Infrastructure

The Company operates on Tier IV-certified servers located in Curaçao, ensuring a high level of infrastructure reliability and security. Regular mandatory backups are performed to ensure data integrity and availability.

A Tier IV data center is the highest classification data center. It helps ensure near-continuous operation, even during maintenance activities or unexpected equipment failures. The ensured availability is **extremely high - 99.995% uptime**. Any single failure (power, cooling, network, UPS, generator, etc.) should not disrupt operations. The facility can continue functioning even if a critical component unexpectedly fails. Equipment can be serviced, repaired, or replaced without shutting down IT systems. Planned maintenance does not require downtime.

The TIER IV data center ensures **redundant infrastructure** (such as multiple independent power paths / cooling systems, redundant UPS system, backup generators with fuel reserves, diverse network connectivity). Therefore, a complete second set of critical infrastructure exists. Because all critical



systems are duplicated and isolated, the likelihood of a single point of failure affecting operations is extremely low.

The SLA with service provider stipulates that:

- 1) The Service Provider critical hosting environments will be available to the Company free of complete environment-wide outages for 100% of the time in any given month
- 2) Hosting Provider provides 24/7 direct support and expertise in any software it provides
- 3) Hosting Provider ensures monitoring in order to analyze availability of TCP/IP based services and applications through its internal monitoring system.
- 4) If hardware failure causes corrupted operating system, data files, or damaged service configurations, Service Provider will restore the system to its original state however possible.
- 5) Users are prohibited from violating or attempting to violate the security of the Service Provider Network. Violations of system or network security may result in civil or criminal liability. These violations include without limitation amongst other:
 - Accessing data not intended for such User or logging into a server or account, which such User is not authorized to access.
 - Attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorization.
 - Attempting to interfere with service to any user, host or network, including, without limitation, via means of overloading, "flooding", "mail bombing" or similar circumstances.
 - Forging any TCP/IP packet header in a network transmission or any part of the header information in any e-mail-based or newsgroup posting.
 - Taking any action in order to obtain services to which such User is not entitled.
 - Addition of IP addresses that have not been specifically assigned to the server.

The hosting provider shall ensure that all Data Center Hosting Services are supported by a number of Core Services (the "Core Services") as listed in the table below. The following Service Levels define the performance parameters and quality of service to be provided for such Core Services.

Service	Definition	Service Level
Power Supply	Operational and redundant electrical power supplies UPS system	A service level of 99.93% for electrical distribution to the data floors
Fire Protection	Specialized smoke system and an Ionisation detection conjunction dedicated fire suppressant system	A service level of 100% protection to the data floors
Air Quality	A designed Down flow Air conditioning.	An average temperature of 21 ° C
Climate Control	System capable of	On the data floor. The

(Climate Control)	maintaining stable temperatures and humidity control within set tolerances	temperature may fluctuate by +/- 4°C. An average humidity of 50% on the data floor. The humidity may fluctuate between 40% and 60%. The temperature and humidity service levels apply in respect of normal operating conditions when measured at the Close Control Units. This service level does not apply to the temperature/humidity within Flutter Networks N.V. cages.
Security	Internal video surveillance and recording system, covering all entrances/exit, main areas and perimeter; full perimeter alarm proximity access card	Security systems will operate on a 24/7/365 basis and will operate to 100% capability
Intelligent Hands	Provision of technical support from Flutter Networks N.V. of onsite technicians who will act as the Client's supervised hands to perform equipment fixes, routine maintenance or troubleshooting	High Severity • Response to first call within one (1) hour or less • Continuous resolution effort on a 24x7 Medium Severity • Response to first call within two (2) hours or less • Continuous resolution effort during Standard Business Hours only Low Severity • Response to first call within four (4) hours or less • Best-effort resolution effort during Standard Business Hours only

10. Responsible Gaming Principles

The Operator has implemented a Responsible Gaming (RG) framework to protect players, prevent gambling-related harm, and ensure regulatory compliance across all brands and gaming verticals.

The Company acts in accordance with the CGA latest Responsible Gaming Policy issued on April 17th, 2025. The Responsible Gaming Policy has been developed by the Company and uploaded to the CGA portal as required. The Company ensures that the policy and the rules are strictly complied with. The Responsible Gaming information and policy can be accessed by players at the website at any time.

Players are guaranteed with that:

- 1) They play in a safe and secure environment;
- 2) Games of Chance are fair and clear to players;
- 3) No Vulnerable Persons can play Games of Chance;
- 4) Players can limit or discontinue their playing of Games of Chance, where such playing threatens to become an addiction for them.

The following technical tools are available at the website to ensure players can self-assess their gaming behavior and vulnerability risks, act independently of the Company and self-set the required limits:

- 1) Deposits limits (option to set daily, weekly and monthly max limits for deposits). Once a limit is reached, further deposits are blocked until the applicable period resets. Where limit changes are requested by the player, increases take effect immediately, while decreases become effective after a 24-hour cooling period.
- 2) Wager limits (option to set daily, weekly and monthly max limits for wager)
- 3) Loss limits (option to set daily, weekly and monthly max loss limits)
- 4) Activity checker (option to set activity checker every 30 minutes, 1 hour and 5 hours. The system displays a pop-up notification at predefined intervals, requesting the user to confirm their presence and activity)
- 5) Cool-off functionality - exclusion from gaming activity for the periods of 1 day, 1 week, 1 month or 3 months. Players can easily activate a cooling-off period through their account settings. Cooling-off is applied to all verticals on the player's selected brand. Players may also opt out of marketing communications. Login remains available during the cooling-off period, while gambling activity is restricted. Account access is automatically restored upon expiry of the selected period.
- 6) Self-exclusion (option to set full self-exclusion without possibility to login for 1 year, 3 years, 5 years, 10 years and permanently). Players can easily activate self-exclusion. Self-exclusion automatically applies to all gaming verticals and is subsequently applied to all brands, blocks player login, and disables marketing communications. Following expiry of the exclusion period, players may request account reactivation upon player confirmation of willingness to do so. The system also supports company-initiated exclusions where required.

The following technical tools are developed to ensure player protection:

- 1) **Player Verification and Protection:** Based on the provided date of birth the system performs age and identity verification during registration to prevent minors from opening or activating accounts.



- 2) **Duplicate account detection:** automatic identification of potentially related accounts by comparing email addresses, personal details, payment instruments, browser fingerprints, and registration or login IP addresses.
- 3) **Global blacklist of self-excluded players:** self-excluded individuals are prevented from accessing existing accounts or creating new accounts across all operators on the platform using the registered email address associated with the self-excluded account.
- 4) **Training of the employees and monitoring** by the frontline staff to detect and take respective measures if vulnerable persons are detected.
- 5) Additionally, players have access to **Responsible Gaming information**, self-assessment tools, safer gambling guidance, and links to professional support organizations across all operator domains.

The Company ensures that its **marketing and advertising activities**, including the offering of bonuses:

- 1) do not encourage excessive gaming;
- 2) are not misleading;
- 3) do not target Vulnerable Persons;
- 4) fully complies with other marketing and advertising rules as specified in the CGA latest Responsible Gaming Policy.

11. Terms and Conditions

The Company's General Terms and Conditions shall be developed in accordance with the guidance issued by the CGA and shall be kept updated at all times. The latest version of the Terms and Conditions is accessible on the website to the players at all times. The latest version of the Terms and Conditions shall also be uploaded to the CGA portal.

The Terms and Conditions at minimum shall include the following information:

1. Company's details
2. Rules on player Registration
3. Rules on amendments and updates of the T&C
4. Record keeping, data privacy and account security
5. Any restrictions applicable
6. Player obligations
7. Account Closure, Suspension, Inactivity, and Withdrawals
8. Company's Non-Financial Institution Status
9. Cancellation or Change to Wagers, Games, and Events
10. Rules on Bonuses and Promotions



11. Rules on Confiscation or Limitation of Winnings
12. Currency for Bets and Prize Money
13. Responsible Gaming rules
14. Dispute Resolution rules
15. Provisions on Fairness and Game Rules

The latest version of the General Terms and Conditions governing the operation and the relationship between the Company and players is attached in Annex 1 “General Terms and Conditions” to this Operation Manual.

12. Dispute Resolution

The Company acts in accordance with the latest CGA Complaints policy issued on June 18th, 2025. The Company’s Complaints Policy has been developed and uploaded to the CGA portal as required. The Company ensures that the policy and the rules are strictly complied with. The Complaints policy and guidelines on submitting the complaint can be accessed by players at the website at any time.

1. A player may file a complaint free of charge within six months after an incident occurred relating to the player’s playing of a Game of Chance by completing and submitting the form available on the website. The form is developed in compliance with the CGA issued guidelines and minimum information required.
2. The Company acknowledges the receipt of a complaint not later than within one week accompanied by an explanation of the way the complaint will be handled.
3. Within four weeks after receiving the complaint, the Company will provide the player either with the final decision or the reason for not processing the complaint. The Responsible Gaming complaints are prioritized and the period of final decision can’t be extended. In other cases the period may be extended for a maximum additional 4 weeks if the Company does not have sufficient information or confirmation to process the complaint earlier.
4. The Company offers the players the opportunity to use alternative dispute resolution, which is CGA-approved and has active agreement with the Company, which is free-of-charge for the players.

13. Critical data storage

The Company shall provide the CGA with the information about the server location where critical data is being kept, including full details of the hosting provider, such as name and address of the hosting provider, relevant server configuration. The information should be provided by submitting relevant agreements with the hosting provider to the CGA.

The Company shall maintain and securely store digital records of all required player, gaming, and financial transaction information. Such records shall be retained and shall be made available



to the Curaçao Gaming Authority (CGA) at all times through infrastructure hosted on servers located in a Tier IV-certified data centre registered in Curaçao.

At least the following minimum critical data shall be maintained on Curacao TIER IV local servers:

1.	Unique player identification code
2.	Player account number
3.	Player's Age
4.	Players residence
5.	ID document type
6.	ID document type number
7.	Daily totals of deposits
8.	Daily totals of withdrawals
9.	Daily totals of wagers
10.	Daily totals of losses
11.	Daily totals of payouts
12.	Daily totals of payouts (bonuses)
13.	Daily totals of blocked winnings
14.	Daily end balance

Appropriate measures shall be implemented to ensure that the integrity, availability, security, and accessibility of such records shall be preserved in accordance with applicable regulatory requirements.



Annex 1 (Terms and conditions)

