

OPERATIONS MANUAL

Product: Online Casino

Industry: Interactive Gaming

Regulating Authority: Curacao Gaming Authority

Operator: CUPWIN B.V.

Revision No.: 1

Adoption Date: 26 May 2026

License Number: OGL/2024/834/0422

OVERVIEW.....	3
1. GAMBLING OPPORTUNITIES, PAYMENTS AND OUTCOME DETERMINATION	3
1.1. Games of Chance	3
1.2. Sportsbook.....	4
1.3. Payment Methods	7
2. TEST METHODS OF QUALITY ASSURANCE	9
2.1. Objective	9
2.2. RNG Implementation Standards	9
2.3. Testing Procedures Implemented by Providers	9
2.4. Third-Party Certification.....	10
3. METHODS OF STORAGE OF PERSONAL DATA AND CRITICAL INFORMATION ABOUT PLAYERS	11
3.1. Data Center and Physical Security.....	11
3.2. Availability and Regulatory Access	11
3.3. Encryption and Data Security.....	11
3.4. Access Control and Audit Trails	12
3.5. Backups and Disaster Recovery	12
3.6. GDPR Compliance and Data Protection Principles.....	12
3.7. Data Retention and Secure Deletion.....	13
4. ELEMENTS OF VISUAL REPRESENTATION	14
4.1. Entertainment Elements	14
4.2. Transparency Elements	14
4.3. Player Protection Elements.....	15
5. MEASURES AGAINST UNAUTHORIZED PARTICIPATION	17
5.1. Age Verification Systems	17
5.2. Jurisdictional Access Control	17
5.3. Account and Identity Validation.....	17
5.4. Device and Session Management.....	18
5.5. Login and Access Security	18
5.6. Fraud and Abuse Prevention.....	18
5.7. Blacklist and Self-Exclusion Enforcement.....	19
6. TECHNICAL INFRASTRUCTURE, RECOVERY OPTIONS.....	20
7. RESPONSIBLE GAMING.....	24
7.1. Policy measures	24
7.2. Instruction and warning measures	24
7.3. RG tools	26
8. TERMS AND CONDITIONS	29
9. DISPUTE RESOLUTION	29
10. METHOD OF STORING DIGITAL RECORD OF CRITICAL INFORMATION	31
10.1. File Contents	31
10.2. Infrastructure	31
11. REVISIONS REGISTER.....	32

OVERVIEW

This Operations Manual (the “**Manual**”) has been prepared in accordance with Article 5.9 of the National Ordinance Containing Rules concerning Games of Chance (“National Ordinance on Games of Chance” or “**NOGC**”) adopted by the Governor of Curaçao on 20.12.2024.

The Manual provides information about the manner and degree of compliance with the provisions laid down in the NOGC, and the rules and restrictions attached to the Gaming License No. OGL/2024/834/0422 held by CUPWIN B.V., a company duly registered in Curaçao.

1. GAMBLING OPPORTUNITIES, PAYMENTS AND OUTCOME DETERMINATION

1.1. Games of Chance

The Operator offers a variety of entertainment activities to players, including games of chance and sports betting opportunities. Below is a non-exhaustive list of games of chance.

1.1.1. Slot Machines

Gameplay: Players spin reels with symbols and aim to match patterns across paylines.

Rules: Each slot game includes a paytable that details winning combinations, bonus features, and multipliers.

Outcome Determination: Spins are determined by an RNG that selects symbol combinations independent of previous spins.

1.1.2. Blackjack

Gameplay: Players aim to achieve a hand value closest to 21 without exceeding it.

Rules: Standard rules apply, including the option to hit, stand, double down, or split. Dealer typically hits on 16 or less and stands on 17 or more.

Outcome Determination: Card distribution is controlled by a shuffled deck algorithm that mimics physical shuffling and is seeded by a secure RNG.

1.1.3. Roulette

Gameplay: Players bet on where a ball will land on a spinning wheel numbered 0–36 (European) or 0–36 plus 00 (American).

Rules: Multiple bet types are available (inside and outside bets).

Outcome Determination: The result (winning number and color) is determined using an RNG simulating a roulette spin.

1.1.4. Video Poker

Gameplay: Player is dealt five cards and can choose which to hold/discard. Replacement cards are drawn.

Rules: Standard poker hand rankings apply for payouts.

Outcome Determination: The dealing and drawing phases are RNG-driven to ensure fairness.

1.1.5. Live Dealer Games

Gameplay: Real human dealers conduct games via video stream.

Rules: Traditional casino rules are applied.

Outcome Determination: Outcomes are determined by physical card draws or spins, with results digitally transmitted for player interaction.

Algorithms of Result Determination

All game results are generated using cryptographically secure Random Number Generators (RNGs). These RNGs:

- Are based on industry-standard algorithms such as Mersenne Twister, Fortuna, or hardware-based entropy sources.
- Are seeded with unpredictable values to prevent pattern prediction.
- Undergo regular audits and statistical testing to ensure fairness.

Each game's outcome generation logic is encapsulated in modular software components that pass compliance testing from recognized laboratories.

1.2. Sportsbook

The Operator offers the following types of bets on the outcome of мфкшщгы sports and e-sports events:

Single bet

A single bet is a bet on a particular outcome. To calculate the return on a single bet, the stake is multiplied by the odds of your selection.

Accumulator bet

An accumulator bet is a bet consisting of several selections on unrelated events. To calculate the return on an accumulator, the stake is multiplied by the corresponding odds of all selections within the accumulator. Should at least one leg fail, the whole bet is lost.

The accumulator cannot contain any related outcomes. Should an accumulator (system) consist of two or more related outcomes, outcomes with the lowest odds will be excluded from the accumulator (system).

Related outcomes (related events) are those when one part of the bet affects another part of the bet.

System bet

A system bet is a bet consisting of several accumulators of the same size on a pre-determined number of outcomes.

The maximum number of accumulators within a system is 184756. The maximum number of outcomes within a system is 20.

To calculate the payout, the returns on all accumulators included in the system are added up.

Chain

A chain consists of several single bets on unrelated outcomes. The stake in each single bet is equal to the stake placed on the very first selection which rolls over with each bet won. The bettor determines the order of bets being settled within a chain and places a bet on the first selection in the chain. For bet settlement purposes, a concept of a "chain account" is used. As each single bet in the chain is settled, the balance on the "chain account" is adjusted accordingly. Initially, the balance equates to the first stake.

As the chain progresses, should the balance on the chain account be less than the pre-determined stake, this remaining balance will be placed on the next selection.

The chain is settled based on the order of bets on the bet slip rather than chronologically. The balance remaining on the "chain account" after all bets have been settled shall be paid. If the balance on the "chain account" drops to zero at any point, the chain is terminated and the bet is deemed lost.

Advancebet

Advancebets are offered to the Customer based on the potential returns from unsettled bets.

Advancebets can be placed either on live sports events or on sports events that are due to start within 48 hours.

When calculating the available Advancebet amount, only bets on events due to start within 48 hours are taken into account.

All bets placed prior to Advancebets and settled within 48 hours after placement of Advancebets will be used to repay Advancebets.

If the payout on settled bets placed prior to placement of Advancebets does not suffice to repay an Advancebet, such Advancebets will be deemed void.

Deposits made after using Advancebets cannot be used to repay such Advancebets.

Multibet

A Multibet is a set of accumulators and single bets. A Multibet may include a Lobby bet or it may not.

A Multibet with a Lobby can be described as an accumulator which includes two bets: a Lobby bet and a system bet consisting of several selections.

A Lobby is an outcome upon which the win of a Multibet depends. A Lobby may be placed as a single bet or as an accumulator.

To create a Multibet, there must be at least three selections on a bet slip (apart from any Lobby). Should the Lobby lose, the whole bet loses. Should the system bet lose, the whole bet loses.

Should the Lobby and one or more legs of the system bet win, the odds of the Lobby shall be multiplied by the odds of the system (depending on how many legs of the system won) and the stake on one leg within the system. If a Lobby is not included in a Multibet, the bet slip shall be treated as a system bet. A Multibet without a Lobby and comprising only of single bets shall be treated as a system bet.

Conditional bet

A conditional bet is a combination of bets (single bets and accumulators) on unrelated outcomes. The bettor may determine at their own discretion the order of the outcomes involved in a conditional bet. All outcomes shall be settled in the order specified on the bet slip. The bettor may determine at their own discretion the stake on each outcome. The stake on each subsequent outcome may not exceed the return from the preceding outcomes. The bettor may also specify only the initial stake. In this event, the stake on each subsequent outcome in the conditional bet will equal the maximum (100%) return from the preceding selection. Should the first selection lose, the conditional bet loses. The settlement of a conditional bet shall be terminated if one of the selections loses and there are no funds left for subsequent stakes.

Anti-Accumulator

An anti-accumulator is the opposite of an accumulator in terms of bet settlement, which means that the bet wins if the relevant accumulator loses. The bet must include two or more selections on unrelated events, and the bet wins should at least one selection lose.

The combined odds of an anti-accumulator are calculated based on the opposite of the winning probability of an accumulator consisting of the same legs.

Lucky

A Lucky bet is a combination of single bets and all associated available accumulators for a specific number of selections. The minimum number of selections is 2, the maximum number of selections is 8.

To get a payout, at least one selection needs to be predicted correctly.

Patent

A Patent involves all the possible accumulators derived from a set number of selections. The minimum number of selections is 3 and the maximum number of selections is 8.

To win, at least one accumulator needs to be predicted correctly (this means a minimum of two selections should be predicted correctly).

1.3. Payment Methods

Players' deposits and withdrawals are processed through a network of recognised Payment Service Providers (PSPs), who provide local payment methods globally under Merchant Agreements with the Operator.

There are various ways of depositing and withdrawing funds from the Customer's account.

The Operator shall follow the following general principles in handling the Players' deposits and withdrawals:

- The Operator shall prioritize due diligence when processing Player deposits and withdrawals.
- All withdrawal requests are processed 24/7.
- If deposits were made through e-payment systems, cash withdrawal requests shall be declined.
- Deposit or withdrawal amounts must be consistent with bets placed (the Customer must place bets with stakes which add up to the sum of all deposits and the bets must have odds of at least 1.1; placing a high volume of bets that have a minimal impact on your balance shall not be taken into account, i.e. bets placed on opposite outcomes in games such as Roulette, Baccarat, Craps and Dice). Permitted

withdrawal amounts shall be calculated based on the amount of the bets placed from any given deposit.

- If the betting account is misused, withdrawals shall be blocked until verification takes place.
- Withdrawing shall only be available using the same payment details that were used for depositing. In case of using different methods to make a deposit, withdrawals should be proportionate to the deposits made using any particular method.
- Deposits and withdrawals must only be made to the details of the betting account holder.

1.4. Software and outcome-determining elements

The Applicant's authorized domains are powered by the software licensed out from a software platform provider branded FERTAMI - a software solution for betting companies with 24/7 stream of data and technical support. The Platform provides betting website operators with a reliable software solution designed to deliver high performance and security. Built on advanced technologies, it offers a diverse range of features, including real-time data updates, support for multiple types of bets, huge selection of sports, flexible customization options etc.

In terms of casino functionality, FERTAMI sources its gaming software from the most advanced and established software developers, such as Mancala, Novomatic, Pragmatic Play, Wintfinity, Zeus and others - and integrates them into the platform.

As far as the sports betting part is concerned, FERTAMI provides a sportsbook platform with a significant capacity for monitoring and betting on a wide range of sporting events - from world-class championships in popular sports to more niche local matches held globally. It also provides extra functionality such as advanced sports stats and analytics in real time, live streaming, visualization and other tools for users.

For the Operator, the platform provides such functionality as CRM, user account management, integrated affiliate program, back office, payment solution integration and other tools.

2. TEST METHODS OF QUALITY ASSURANCE

2.1. Objective

Quality assurance of the i-gaming business consists in ensuring that the cornerstone of the gaming software used by the Operator - random number generator (RNG) - is truly fair. To ensure fairness, unpredictability, and compliance, the RNG systems used in the platform are rigorously tested using statistical methods and third-party certification processes.

2.2. RNG Implementation Standards

RNGs used on the Website must conform to international standards such as:

ISO/IEC 18031: Security techniques for random bit generation.

GLI-19/GLI-11: Guidelines from Gaming Laboratories International for interactive and RNG-based gaming systems.

2.3. Testing Procedures Implemented by Providers

Frequency Tests

Ensures uniform distribution of results.

Compares observed vs. expected frequencies over large sample sizes.

Runs Test

Examines sequences for expected variation.

Identifies abnormal patterns that could indicate bias.

Autocorrelation Test

Detects any correlation between successive numbers.

RNG output should show zero correlation for randomness.

Chi-Square Goodness-of-Fit Test

Evaluates the distribution of generated numbers against a theoretically uniform distribution.

Entropy Measurement

Measures the randomness or disorder in the RNG outputs. Higher entropy indicates more unpredictability.

2.4. Third-Party Certification

Before integration to the Website, all software providers must submit a valid RNG certificate issued by independent laboratories upon performing relevant technical audits:

eCOGRA, iTech Labs, GLI, and BMM Testlabs are recognized authorities that verify RNG fairness.

Certification includes:

- RNG output sampling and analysis
- Source code review
- Seed management practices
- Change management and logging mechanisms

Certified RNGs are re-evaluated regularly to maintain accreditation and are accompanied by official reports available for review upon regulatory request.

3. METHODS OF STORAGE OF PERSONAL DATA AND CRITICAL INFORMATION ABOUT PLAYERS

3.1. Data Center and Physical Security

All player personal records – including name, address, identification, payment, gameplay and transaction history, and communications – are hosted on servers in a Curaçao-registered Tier-IV certified data center. A Tier-IV “fault-tolerant” design uses fully redundant power, cooling, and networking (2N+1 architecture) so that no single failure can interrupt service. This ensures near-100% uptime and supports continuous operation. The facility employs strict physical security (24/7 monitoring, biometric access controls, etc.) and environmental protections (climate control, fire suppression) to safeguard the hardware and data against unauthorized access or damage.

3.2. Availability and Regulatory Access

Systems are engineered for uninterrupted availability so that the Curaçao Gaming Authority (CGA) can access records at any time. Redundant servers and network links provide 24/7 operation, and real-time replication ensures that current and historical data remain online and readable. In practice, this architecture achieves approximately 99.995% uptime for all critical systems. Should one component fail, failover mechanisms immediately shift operations to backups, ensuring regulators can retrieve the required data without delay.

3.3. Encryption and Data Security

Encryption at Rest: All stored personal data are encrypted on disk using strong algorithms (e.g. AES-256). This means that if physical storage media were compromised, the data remain unreadable without the encryption keys. Encryption keys are themselves stored securely with strict key-management policies.

Encryption in Transit: All data exchanged over networks (e.g. between servers, applications, or player devices) use secure channels (TLS/SSL) to encrypt data in flight. In line with Curaçao technical standards, “all data transmitted between critical components shall utilize an appropriate level of cryptography” . This protects data integrity and confidentiality during transfer and prevents interception or tampering by unauthorized parties.

Data Integrity: Cryptographic checks (hashes, digital signatures) are used to detect any unauthorized alteration of records. Routine integrity checks and monitoring ensure that any corruption or tampering is immediately flagged and investigated.

3.4. Access Control and Audit Trails

Role-Based Access Control: Access to the system is tightly controlled by user role. Each administrator or employee is granted only the privileges needed for their job function. For example, help desk staff cannot view financial transaction logs, and auditors have read-only views. As one security overview explains, access control is like “a bouncer at a club, only letting in authorized individuals” . All user actions require unique credentials, and administrators use multi-factor authentication and frequent password changes for critical accounts.

Audit Logging: Every access and change to personal data is automatically logged with date/time, user ID, and action details. These logs are tamper-resistant and reviewed regularly. Maintaining detailed audit trails is a standard security practice (e.g. ISO 27001) and helps detect unauthorized access. In fact, audit logs enable complete accountability: if an incident occurs, logs show “who did what and when” in the system . Log retention is also managed securely (see Data Retention below) to preserve evidence and enable regulator review.

3.5. Backups and Disaster Recovery

All critical personal data are backed up frequently and comprehensively. Daily full backups (with hourly transaction logs) are performed and stored off-site. Backup copies are themselves encrypted and verified to ensure they can be reliably restored. Industry guidelines note that “regular backups are necessary to safeguard your data from hardware malfunctions and hacking attempts and to enable quick recovery” . Accordingly, the operator uses automated backup scheduling, with at least one copy kept in a geographically separate location. Backup restoration procedures are tested periodically to confirm that, in the event of a system failure or data loss, services can be restored rapidly with minimal downtime. This redundant backup strategy guarantees business continuity and protects against data loss.

3.6. GDPR Compliance and Data Protection Principles

The data storage methods adhere to both Curaçao regulations and EU GDPR principles:

Data Minimization & Purpose Limitation: The system collects only the personal data strictly needed for gaming, account administration, and AML/KYC compliance . Forms and databases are designed to avoid superfluous fields. Data are used only for the purposes disclosed to the player at collection.

Subject Access and Erasure Rights: Under GDPR, players have the right to access their personal information and to request correction or deletion. The operator has processes to respond to such requests within the required timeframe. GDPR

explicitly grants data subjects the “right of access” and “right to erasure” , and our procedures honor these rights (for example, by producing data reports upon request or securely deleting an account’s data if permitted).

Data Protection Impact Assessments (DPIAs): High-risk processing activities (such as introducing new KYC technology or large-scale profiling) are assessed via DPIAs. The GDPR mandates a DPIA “where ... processing is likely to result in a high risk to ... rights and freedoms” . Our DPO oversees this process to ensure that privacy risks are identified and mitigated in advance.

Accountability and Documentation: All security controls, policies, training, and audit results are documented. This provides evidence of compliance and enables the operator to demonstrate adherence to CGA rules and GDPR requirements (Accountability principle). Regular internal audits verify that the data handling processes remain compliant and up to date.

3.7. Data Retention and Secure Deletion

Personal data are retained only for as long as legally and operationally required. Retention periods are defined by law (e.g. Curaçao AML regulations typically require at least 5–7 years for transaction records) and by business need. After these periods expire, or when a player account is closed, data are permanently erased or rendered anonymous. Secure deletion methods include cryptographic erasure (e.g. destroying encryption keys) and multiple-pass data wiping of storage media. Physical drives that leave service are treated with data-sanitization procedures: approved tools overwrite data to industry standards, and drives may be degaussed or physically shredded to ensure no information can be recovered . These deletion practices fulfill GDPR’s storage limitation principle: personal data “must not be kept longer than necessary” for the purposes collected . All disposal actions are logged, and certificates of destruction are retained where applicable.

4. ELEMENTS OF VISUAL REPRESENTATION

The visual representation and its design elements of the online casino serve three main purposes:

- Entertainment - creating an exciting and convenient experience for the Player to make the Operator stand out among the competition.
- Transparency - informing the player of all applicable Terms & Conditions of the service offered to them, their rights and obligations, ways to protect their rights and reach out to the Operator, the ADR provider.
- Access to Functionality - making all the tools of the website available to the user, stopping ineligible players from using the service and aiding vulnerable persons in getting help if needed.

While each Section of the website or mobile application (where applicable) has its own elements of design that can be added, moved and replaced as per the Operator's vision, certain elements shall be readily available to visitors regardless of the subpage they are currently visiting - which is the subject of this section.

4.1. Entertainment Elements

A. Games/ Casino Games etc.

A player chooses a game which is opened in a separate window with an active user interface, design elements and animation depending on the game. A player cannot start the game unless they are registered with the Operator. Header and footer are visible at all times.

B. Sports Betting

A bettor chooses a sport he is interested in and further proceeds to the match of his preference. Then they choose an outcome they want to bet on and proceed to betting. A bettor cannot place a bet unless they are registered. Header and footer are visible at all times.

4.2. Transparency Elements

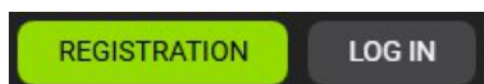
The elements related to transparency must be visible at all times to all visitors of the website.

Header contents:

- direct links to each of the major kinds of betting:



- access to the Player account:



- casino brand logo
- timezone and language preferences



Footer contents:

- Terms and Conditions with direct links to both the whole text and each major section
- direct links to social media
- legal information about the Operator, all its relevant subsidiaries and license
- responsible gaming warning
- direct link to General Terms and Definitions
- i-frame CGA validator seal implemented as per the CGA instructions to ensure that the validity of the license is updated in real time



- contact details of the Operator
- links to mobile application and mobile version
- date and time mark

4.3. Player Protection Elements

These include the standard registration and login form which must be completed by each potential user and the basic tools which can be accessed via the Personal profile button in the header:

- Funds management capabilities
- Activity history
- Information on special offers and bonuses
- Access to customer support service
- Profile management and security
- Responsible Gambling tools

5. MEASURES AGAINST UNAUTHORIZED PARTICIPATION

To uphold the integrity of the platform, comply with regulatory obligations under the Curacao license, and protect vulnerable individuals, the Operator has implemented a comprehensive set of technical measures aimed at preventing unauthorized participation. These measures cover age verification, jurisdictional restrictions, account validation, system monitoring, and fraud detection.

5.1. Age Verification Systems

- **Mandatory DOB Input:** During the registration process, users are required to enter their full date of birth. The system automatically verifies that the user is at least 18 years of age.
- **Automated Document Verification:** Upon registration or before first withdrawal, the platform may request a valid government-issued ID and perform automated checks through third-party KYC providers to validate age and identity.
- **Manual Review:** In cases of ambiguity or failed automatic checks, the Compliance Department manually reviews submitted documents to confirm the user's age.
- **Blocking Minors:** If a user is found to be underage at any stage, their account is permanently disabled, and all transactions are voided as per the Terms and Conditions.

5.2. Jurisdictional Access Control

- **Geo-IP Filtering:** The platform uses real-time IP detection to determine a user's location. Access is restricted or blocked for users from blacklisted countries and jurisdictions where gambling is prohibited or unlicensed.
- **VPN and Proxy Detection:** Advanced tools are used to identify and block users attempting to access the platform via VPNs, proxies, or Tor networks.
- **Dynamic Country Banning:** Based on regulatory changes, the list of restricted jurisdictions is dynamically updated, and access from new restricted territories is blocked automatically.

5.3. Account and Identity Validation

- **Email and Phone Verification:** New users must verify both their email and phone number through one-time password (OTP) confirmation.

- **Unique User Constraints:** The system enforces the “one user, one account” policy by identifying duplicate registrations through device fingerprinting, cookie checks, email similarity detection, and shared IP addresses.
- **KYC Triggers:** Users are prompted to complete the Know Your Customer (KYC) process under the following conditions:
 - Upon reaching cumulative deposit thresholds;
 - Before the first withdrawal;
 - If suspicious behavior is detected;
 - As part of routine periodic checks.

5.4. Device and Session Management

- **Device Fingerprinting:** The system collects device-specific data (OS, browser, resolution, plugins) to build a fingerprint. Attempts to create multiple accounts from the same device are flagged.
- **Concurrent Session Control:** Users are generally limited to one active session per account. Logins from new devices or locations prompt alerts and may trigger secondary authentication.
- **Session Timeouts and Auto-Logout:** Sessions are automatically terminated after a period of inactivity to prevent unauthorized use.

5.5. Login and Access Security

- **Multi-Factor Authentication (MFA):** Users are encouraged (or optionally required) to activate MFA via authenticator apps or SMS-based OTP.
- **Login Attempt Monitoring:** Failed login attempts are tracked. Repeated failures result in account lockout and notification to the security team.
- **CAPTCHA Integration:** CAPTCHA systems are implemented on login and registration forms to prevent bot activity and automated abuse.

5.6. Fraud and Abuse Prevention

- **Automated Behavior Monitoring:** Risk management tools monitor user activity (betting patterns, login times, transaction behavior) to identify anomalies indicating possible unauthorized use.
- **Real-Time Alerts:** Suspicious actions, such as frequent IP/location changes, rapid deposit/withdrawal attempts, or use of known fraudulent BINs, trigger immediate alerts to the Fraud Prevention Team.

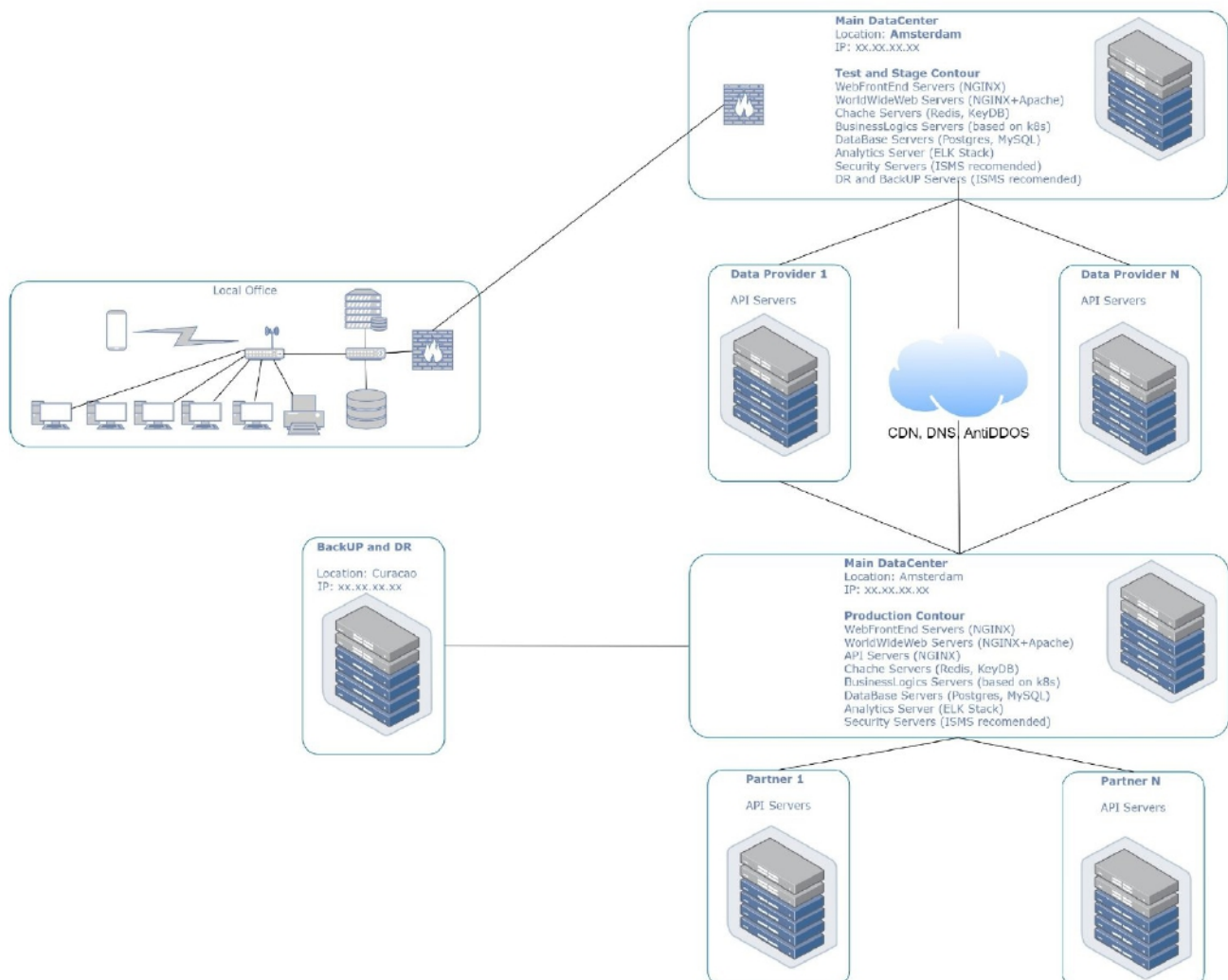
- **Transaction Limits & Velocity Controls:** The platform applies configurable limits on deposit and withdrawal frequencies to reduce the risk of automated abuse or account takeovers.

5.7. Blacklist and Self-Exclusion Enforcement

- **Self-Exclusion Databases:** Users who choose to self-exclude are blocked at the account level. They cannot log in, deposit, or participate in any games.
- **Internal Blacklists:** Suspicious users (e.g., chargeback fraud, multi-accounting) are added to an internal blacklist.

6. TECHNICAL INFRASTRUCTURE, RECOVERY OPTIONS

Company's technical infrastructure includes a primary on-site data centre at the head office, corporate servers for critical applications, and integrated backup systems. The data centre houses core servers (e.g. file, database, application servers) with redundant network and power supplies. Uninterruptible Power Supplies (UPS) and standby generators provide power continuity. Key components – including routers, switches and a firewall – have failover configurations to ensure resilience. Critical servers and data are backed up daily to an off-site location and secure cloud storage. Routine testing of these backups ensures rapid restoration if needed.



- **Data Centres & Servers:** The main on-premises data centre is fully equipped with cooling, power redundancy, and secure racks. A secondary (off-site) backup facility or cloud service holds replicated data. All critical servers (finance, HR, CRM, etc.) are virtualised where possible, allowing quick redeployment on alternate hardware.

- **Networking Equipment:** Core routers and switches are configured with failover protocols. Redundant internet connections (primary and secondary ISPs) allow automatic switchover to keep external connectivity alive. Network diagrams and configuration backups are maintained for rapid re-establishment of service.
- **Backup Systems:** Data backup includes onsite disk-based backups and encrypted offsite archives. Essential backups cover application data, system images, and configuration files. Backup generators (diesel or gas) maintain power to critical infrastructure during outages .

IT RECOVERY PROCESS

In a disaster, Company's IT recovery plan follows a step-by-step process covering hardware, software, and communications systems. Recovery priorities and responsibilities are clearly defined so that systems can be restored in order of criticality. The IT team (or designated external support) will implement each of the following:

- **Hardware Recovery:** Identify damaged equipment and request replacements or spares. Maintain contact lists for hardware vendors and support services. For failed servers, replace defective components using on-site spares (hard drives, memory, etc.) or swap in pre-configured standby servers. Ensure power supplies, UPS units, and generators are operational.
- **Software & Data Restoration:** Reinstall operating systems and essential applications from saved images or media. Configure systems using documented procedures. Restore data from the latest off-site backups. Verify applications (ERP, email server, databases) are functioning with current data. Apply any critical patches or updates as part of the rebuild.
- **Internet & Network Services:** In the event of primary ISP failure, switch to the secondary internet connection. If office networking equipment is lost, re-establish VPN tunnels so remote sites and employees can connect securely. Network monitoring and management tools should be reset or relocated to ensure visibility of restored services.
- **Email and Phone Systems:** If the on-site email server is unavailable, shift to the cloud-hosted email system (e.g. Office 365) that remains accessible. For telephony, enable call forwarding; configure the VoIP/PBX system to route calls to mobile phones or a backup provider. Ensure voicemail greetings are updated to inform callers of any change in operations.
- **Servers and Workstations:** Bring critical servers online first (file servers, domain controllers, core databases). Once server infrastructure is stable, focus on workstations. Staff laptops and desktops should have network imaging software to allow rapid OS and application reload. Provide employees with instructions for securely accessing company resources (VPN, remote desktop, SaaS platforms) if local machines are lost.

Throughout the recovery, documented checklists guide technicians on step-by-step tasks (e.g. “Power on backup server → verify RAID array health → restore database from latest backup” etc.). Responsibility for each system is assigned in advance (for example, IT Manager – network; Systems Admin – servers; Helpdesk – desktop support).

OFFICE LOCATION RECOVERY OPTIONS

If the primary office building is unusable, Company has multiple fallback workplace arrangements:

- **Director’s Home Office:** The director’s residence is pre-approved as an emergency alternate site. It is equipped with a secured network connection, power backup (UPS), and configured as a mini data centre for critical operations. Essential IT equipment (workstation, router, printer) is installed and tested periodically. Staff can report here on short notice if needed.
- **Serviced Offices or Rented Space:** Agreements are in place with local serviced-office providers. Within 24–48 hours, a temporary office can be furnished with desks, chairs and internet service. The IT team maintains portable network gear and spare laptops to set up quickly in these locations. A list of providers and contact numbers is kept updated.
- **Remote Work (Telecommuting):** All employees are trained and enabled to work remotely. Each staff member has a remote-access laptop and credentials for VPN or secure cloud services. Standard remote-work guidelines (VPN use, data security) apply. If travel to any physical site is impossible, staff continue operations from their home offices. The recovery plan ensures that core systems (email, file sharing, teleconferencing) are fully accessible remotely.

Each alternative location plan includes logistical details: addresses, contact persons, arrival instructions, and any required access codes. Decision criteria (e.g. “Director’s home if local disaster; serviced office if extended outage”) are specified so that team members know where to go without delay.

STAFF COMMUNICATION & ACTION PLAN

Clear communication and defined roles are critical during a disaster. Company’s plan ensures all staff know who to contact and how to act:

- **Notification Procedures:** Upon a disaster event, the Incident Commander (e.g. CEO or appointed manager) activates the emergency plan. The Communications Lead calls or texts all staff using a pre-established call-tree or group messaging app. Initial messages convey the nature of the incident and immediate instructions (e.g. “Evacuate building; check in by phone”).

- **Roles and Responsibilities:** Key personnel are assigned duties in advance. For example, IT leads recovery of systems, Facilities Manager secures premises, and Office Manager handles logistics (e.g. arranging the backup site, notifying clients/suppliers). Contact lists for all staff include home phone, mobile, and alternate contacts. Each person confirms their own and dependent's safety before focusing on recovery tasks.
- **Communication Channels:** Multiple channels are used to ensure reachability. Primary communication is via corporate email and phone, but if these fail, backup methods include SMS/text alerts, WhatsApp or Slack groups, and social media/private forums as needed. The plan specifies a central "status board" (online or physical) for updates on recovery progress and assignments.
- **Information Updates:** Regular briefings are scheduled (via conference call or group chat). Updates include what systems are up/down, where staff should work from, and who to call for help. Critical announcements (e.g. emergency contact numbers, relief services) are distributed by the Crisis Communications team. All communication templates (message scripts, holding statements for media, etc.) are prepared in advance.

By following these procedures, Company ensures employees stay informed and can concentrate on essential work. The focus remains on safety first, then on restoring key functions so the business can continue operating through the disruption.

7. RESPONSIBLE GAMING

The industry's best practices and regulatory requirements dictate that the Operator must be the cornerstone of protecting vulnerable individuals from adverse effects of gambling.

The RG policy is aimed at protecting Vulnerable Persons, promoting responsible gambling as well as preventing and mitigating problem gambling patterns. The Operator does this by implementing Responsible Gaming (RG) policies, tools and procedures.

A Vulnerable Person is defined as having one or more of the following traits:

- Under eighteen years of age.
- Has no, or insufficient, control over his or her gambling behaviour, because of which he or she is, or threatens to become, addicted to one or more Games of Chance and, as a result, may cause harm to himself or herself or to other people.
- Has been banned from playing any Game of Chance either by force or at his or her own request.
- Has been declared bankrupt.

This creates obligations for the Operator, who implements the following steps in relation to RG.

7.1. Policy measures

- Ban on underage gambling (for persons under the age of 18).
- Ban on advertising gambling products and services to minors or vulnerable people.
- Ensuring that advertising, sponsorship, and marketing activities do not contain any information aimed at attracting underage or vulnerable persons.

7.2. Instruction and warning measures

- Instructing users on risks of gambling
- Informing users that gambling is entertainment, not a way of creating wealth
- Warning users against sharing authorized devices, credentials and payment details with other persons.

Apart from messages published across the website and user profile, an example of such instruction, the users are offered to pass a self-assessment to test the level of their gambling addiction:

—

Please answer "Yes" or "No" to the questions below:

1. *Did you ever lose time from work or school due to gambling?*

2. *Has gambling ever made your home life unhappy?*
3. *Did gambling affect your reputation?*
4. *Have you ever felt remorse after gambling?*
5. *Did you ever gamble to get money with which to pay debts or otherwise solve financial difficulties?*
6. *Did gambling cause a decrease in your ambition or efficiency?*
7. *After losing did you feel you must return as soon as possible and win back your losses?*
8. *After a win did you have a strong urge to return and win more?*
9. *Did you often gamble until all your money was gone?*
10. *Did you ever borrow to finance your gambling?*
11. *Have you ever sold anything to finance gambling?*
12. *Were you reluctant to use "gambling money" for normal expenditures?*
13. *Did gambling make you careless of the welfare of yourself or your family?*
14. *Did you ever gamble longer than you had planned?*
15. *Have you ever gambled to escape worry, trouble, boredom, loneliness, grief or loss?*
16. *Have you ever committed, or considered committing, an illegal act to finance gambling?*
17. *Did gambling cause you to have difficulty in sleeping?*
18. *Do arguments, disappointments or frustrations create within you an urge to gamble?*
19. *Did you ever have an urge to celebrate any good fortune by a few hours of gambling?*
20. *Have you ever considered self-destruction or suicide as a result of your gambling?*

If you answered "Yes" to any of the questions above, then it is likely that you have a gambling problem.

—

Also, the Operator informs users on third-party RG solutions and help organizations in the respective section of the Terms & Conditions.

Web-tools

betblocker.com

gamblock.com

gamban.com

Additional Support

Support organizations available to offer guidance and assistance:

Gamblers Anonymous

Website: <https://gamblersanonymous.org/ga/>

Gambling Therapy

Website: <https://www.gamblingtherapy.org/>

Contact: support@gamblingtherapy.org

GamCare

Website: <https://www.gamcare.org.uk/>

Live chat: <https://www.gamcare.org.uk/get-support/talk-to-us-now/#>

Gambleaware:

Website: <https://www.gambleaware.org/>

Contact: contact@gambleaware.org

7.3. RG tools

The Operator implements comprehensive RG tools accessible immediately from the user's profile and by streamlining customer service.

Cooling-off:

The Cooling-off tool allows user to suspend gaming activity for a selected period.

During this time, user will not be able to:

- deposit into user account,
- place bets,
- participate in promotions.

During this time, user will be able to:

- access user account,
- withdraw funds from user account,

User can choose one of the following periods:

- 24 hours
- 7 days
- 1 month
- 3 months

After the specified period expires, access to all platform functions will be restored automatically.

Users can exclude themselves from any marketing communications during the cooling-off period.

Self-exclusion

With the Self-exclusion tool, user will irrevocably lose access to the following functions for the selected period:

- accessing user account
- depositing,
- placing bets,
- participating in promotions
- creating new accounts.

User can choose one of the following periods:

- 1 year
- 3 years
- 5 years
- 10 years
- for life

The decision to self-exclude cannot be reversed, and the user who used this option has to send us a written request to reactivate their account after the expiry of the restriction period.

Any attempt to create a new Account during Self Exclusion is a violation of Terms of Service and may result in the permanent ban of the original account.

The user must complete any tournaments (for example poker tournament) that is in-running at the time of self-exclusion.

Contributions to progressive jackpots that the user made through gameplay prior to the self-exclusion request remain in place, but they will not be eligible to participate in the jackpot after the self-exclusion comes into effect.

Deposit Limits

The Deposit Limit tool limits the total amount a user can deposit over a defined period of time. Once the limit has been reached, further deposits will not be available until the end of the specified period.

Decreases in the limit will take effect immediately and increases only take place after 7 days.

A user can choose one of the following periods:

- daily
- weekly
- monthly

Any resolved or unresolved wager made prior to the deposit limit being set in place remains unaffected by the said limit.

Other Concerns

The Operator maintains a Customer Service via email and live chat for an increased flexibility of the RG options available to the user - like setting limits on their online activity, getting clarifications on other RG tools, raising concerns or just reaching out for help.

8. TERMS AND CONDITIONS

The most recent text of the General Terms & Conditions used by the Operator can be found at the link below:

<https://winebet.com/en/information/rules/terms/1>

9. DISPUTE RESOLUTION

The Operator follows the industry's best practices and regulatory requirements to ensure that all user disputes are handled in a transparent, fair, and timely manner. All users have the right to lodge a complaint concerning any aspect of their interaction with the Company, including but not limited to account activity, payments, promotions, verification, game outcomes, responsible gaming, and regulatory matters.

All complaints will be reviewed objectively, and the user will not be disadvantaged for initiating a complaint in good faith. Each complaint follows a similar lifecycle:

1. The user submits a complaint

Customers may submit a complaint free of charge within six (6) months of the incident in question. To file a complaint, the Customer must complete the complaint form available in PDF format at a respective link accessible from a respective Section of the T&C, and submit the completed form by email to the Support Service specified in the same section.

The complaint submission includes:

- full name and registered address of the Customer;
- Account ID;
- date of the incident or dispute;
- a clear description of the issue, including any relevant documentation or evidence;
- preferred language (English or another language of the target market).

2. The Operator accepts the complaint:

Upon receiving a complaint, the Operator will:

- acknowledge receipt within seven (7) days via email or another preferred communication method;
- provide an explanation of the review process and expected resolution timelines.

The Operator aims to issue a final response within four (4) weeks of receiving the complaint. In complex cases, this period may be extended once for up to an additional four (4) weeks, with prior notice and explanation to the Customer.

Complaints related to responsible gaming will be prioritized and, where possible, resolved within five (5) business days. If more time is needed, the Customer will be informed, and the delay will not exceed two (2) weeks.

3. The Operator resolves the complaint

All decisions will be communicated in writing and will include either:

- A clear explanation of the final resolution and its justification; or
- A reasoned explanation for not handling the complaint (e.g., insufficient information).

3.A The user escalates the Complaint to Alternative Dispute Resolution (ADR)

If a complaint is not resolved to the Customer's satisfaction, the matter may be escalated to an independent Alternative Dispute Resolution (ADR) body, which will review the dispute impartially.

ADR services are provided free of charge to the Customer.

The ADR service resolves the complaint, and the resolution is considered final for both the user and the Operator this finalizing the complaint lifecycle.

Record-Keeping and Reporting

The Company maintains a detailed record of all received complaints for a minimum period of five (5) years, including:

- Resolved complaints (upheld or rejected);
- Unresolved complaints;
- Complaints escalated to ADR or legal action.
- The Company submits regular reports on complaint statistics and outcomes to the appropriate regulatory body, as required.

10. METHOD OF STORING DIGITAL RECORD OF CRITICAL INFORMATION

The Operator shall keep a digital record of players, player gaming transactions and their financials.

10.1. File Contents

The record shall be uploaded from the Operator's platform as a file with .csv or .xlsx extension on a regular basis as per the CGA requirements.

The record must include the following information:

- Player Account ID
- Player Account Country
- Transaction ID
- Date of Transaction
- Currency of Transaction
- Transaction Amount
- Payment Method

The digital record is to be retained for 5 years.

10.2. Infrastructure

The records shall be kept on a server located in a Curacao-based Tier-IV certified datacenter. The server shall be encrypted to only be accessible with login and password or by using a similar authentication method.

The server shall be made available to the CGA at all times by providing respective access credentials.

Otherwise, the digital record must be treated by the Operator's employees and hosting provider as personal data, as per Art. 4 (1) of the Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

For more information, refer to section 3 of this Operations Manual.

11. REVISIONS REGISTER

Revision No.	Date	List of changes
1	26 May 2026	

For and on behalf of CUPWIN B.V.:

Position: Managing Director

Name: Tetiana Boiko

Signature: _____

Date: 26 May 2026

