

HORIZONIX CORP N.V.

*Licensed by the Curaçao Gaming Authority since 19/Dec/2025
to offer games of chance under license number OGL/2024/1944/1124*

OPERATIONS MANUAL

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

Document Version: 1.0

Effective Date: July 1, 2026

Document Status: Confidential

COMPANY INFORMATION

Full Company Name: Horizonix Corp N.V.

Registration Number: 166811

Registered Address: Hanchi Snoa 19, TRIAS Building, Willemstad, Curaçao

TABLE OF CONTENTS

Operations Manual Requirements

Section 1 — Description of Games of Chance Offered, Payment Possibilities, Bet Amounts, Payouts, Software, and Outcome-Determining Elements

Section 2 — Description of Periodically Used Test Methods for Quality Monitoring

Section 3 — The Way of Storing Players' Personal Data and Other Details

Section 4 — Description of Visual Elements Shown to Players Through the Gaming Website or Other Software Application

Section 5 — Description of Technical Measures Put in Place to Prevent the Admission of Banned Natural Persons

Section 6 — Diagram of the Technical Infrastructure and Description of Restoration Possibilities in the Event of a Technical Emergency

Section 7 — Description of How the Principles of Responsible Gaming Have Been Implemented in the Operation

Section 8 — The Most Recent Text of the General Terms and Conditions Used by the Operation

Section 9 — Description of How the Licensee Settles Disputes with Players

Section 10 — The Digital Records Kept of Specific Critical Information About Players, Their Gaming Transactions, and Their Financial Transactions

Annexes

Annex 1 — General Terms and Conditions of Horizonix Corp N.V. (gravira.com)

Annex 2 — Responsible Gaming Policy

Annex 3 — Player Complaints Policy and Complaint Submission Form

Annex 4 — AML/CTF Policy and KYC Policy

Section 1. Description of Games of Chance, Payment Possibilities, Bet Amounts, Payouts, Software, and Outcome-Determining Elements

1. Overview of Gaming Operations

Horizonix Corp N.V. (the "Company" and/or "Horizonix") operates an online gaming platform accessible at authorised Websites (the "Website" and/or "Websites"), offering a comprehensive range of licensed games of chance to registered players.

The Company currently operates exclusively under the Gravira brand, through its single operational domain, gravira.com. The domain vashbet.com is registered to the Company but is not currently operational: it carries no visual design, branding, or player-facing content, and remains under development. No games of chance are offered, and no player accounts can be registered or accessed, through vashbet.com at this time. Should the Company launch vashbet.com as an active, player-facing brand in the future, the Company will update this Operations Manual accordingly prior to launch, including all brand-specific elements relevant to the new domain.

Horizonix collaborates with an independent iGaming software provider, which acts as its core platform provider (the "Platform"), which also facilitates access to a broad portfolio of licensed third-party gaming content. Through the Platform infrastructure and integrations, the Company is able to aggregate and offer a diverse range of games from established studios, enabling a comprehensive selection of high-quality products to be delivered through a single, centrally managed platform. This setup supports a consistent, engaging player experience and allows Horizonix to manage game content, player accounts, transactions, and operational controls in a streamlined manner.

2. Games of Chance Offered

The Company's gaming catalog is made available through the Platform and encompasses the following categories of games of chance:

2.1 Slots (RNG-Based). Online slot games feature a set of reels — typically three or five — with various symbols. Outcomes are determined by a certified Random Number Generator ("RNG") embedded in each game's software. Players place a wager and initiate a spin; the RNG generates a random outcome determining whether a winning symbol combination is achieved. Winning combinations and corresponding payout multipliers are defined in each game's paytable, which is accessible to players prior to and during play.

2.2 Table Games (RNG-Based). The platform offers RNG-based digital versions of classic table games, including but not limited to blackjack, roulette, baccarat, and poker variants. Game outcomes are determined by certified RNG software that replicates the statistical distribution of outcomes equivalent to physical games of chance. Rules, bet types, and payout ratios are defined by each game's configuration and made available to players within the game interface.

2.3 Live Dealer Games. Live dealer games are offered as real-time video-streamed sessions hosted by human dealers or croupiers at dedicated studio facilities operated by third-party providers. Game outcomes are determined by physical means — card draws, roulette wheel spins, or dice rolls — conducted on-camera and in real time. The results are digitally captured and transmitted to the platform. Players interact with the game through a graphical interface that reflects live game state in real time.



2.4 Virtual Sports. Virtual sports products simulate sporting events (e.g., football, horse racing, greyhound racing) through computer-generated graphics. Outcomes are determined by a certified RNG, with results produced at regular intervals independent of real-world sporting events.

2.5 Bingo. Bingo games are offered in digital format, where numbers are drawn by a certified RNG. Players are allocated cards with pre-assigned numbers and win based on completing predefined patterns.

2.6 Instant Games. Instant win games offer immediate outcomes determined by a certified RNG upon the player initiating a game round. These include scratch-card style and other rapid-play formats.

In total, the Company's portfolio is sourced from over 140 licensed game providers. All game providers are selected based on their regulatory standing, technical certification standards, and demonstrated compliance with applicable international gambling regulations.

2.7 Critical supplier control. Before any game provider, live dealer studio, sportsbook/odds provider, game aggregator, payment provider, hosting provider, or other critical service provider is used in production, the Company must complete risk-based supplier due diligence, verify applicable licences/certifications, confirm contractual obligations for availability, information security, incident notification, certification maintenance, data protection and regulatory cooperation, and record the supplier in the Company's Critical Supplier Register. From the date on which CGA supplier registration requirements become fully enforceable, the Company must only engage critical suppliers that are licensed or registered with the CGA where required.

3. Software and Technical Infrastructure

All games are integrated into the Platform via a standardized API. The platform's technological stack includes MongoDB and PostgreSQL for data storage, Apache Kafka for real-time data stream management, Redis for caching, and JavaScript, Java, and Scala as primary programming languages.

The front-end player interface is built on React and React Native, delivering a consistent experience across web browsers and mobile devices. The back-end is developed in Python, supported by Aiohttp, NATS messaging, Elasticsearch, and PostgreSQL for structured transaction and player data.

The Platform, as content distributor and platform operator, ensures all integrated games are subject to ongoing technical testing prior to and following integration, to verify correct operation, RNG integrity, payout accuracy, and compliance with applicable regulatory standards.

4. Outcome-Determining Elements

Outcomes in all RNG-based games — including slots, table games, virtual sports, bingo, and instant games — are determined exclusively by certified random number generator software embedded in the game modules provided by licensed third-party studios. These RNG systems are independently tested and certified by recognized testing laboratories (such as GLI, BMM, eCOGRA, or equivalent) in accordance with applicable gaming standards.

Outcomes in live dealer games are determined by physical randomization conducted in real time by a human dealer, with results captured and communicated digitally to the player.

No outcome in any game offered on the platform is influenced by the Company's operational staff, platform configuration, or any mechanism other than the certified RNG or physical process described above.

5. Payment Possibilities



The Company facilitates deposits and withdrawals through a range of payment methods integrated via third-party payment service providers ("PSPs"). Accepted payment methods include, but are not limited to, bank cards (Visa, Mastercard), electronic wallets, bank transfers, and cryptocurrency payment solutions, subject to availability by jurisdiction and player verification status.

All financial transactions are processed in real time through the Platform payment processing module, which applies encryption, transaction authorization, fraud risk scoring, and real-time balance updates. Deposit and withdrawal limits, available currencies, and supported payment methods are detailed in the relevant Terms and Conditions and/or policies of the Company and in the relevant sections of the player interface.

6. Bet Amounts and Payouts

Minimum and maximum bet amounts vary by game type, game variant, and game provider configuration. Applicable bet limits for each game are displayed within the game interface prior to and during play. For live dealer games, table minimums and maximums are displayed in the lobby and updated in real time.

Payout ratios (Return to Player, "RTP") for each RNG-based game are established by the respective game provider, independently certified, and disclosed to players in the game's information section. Live dealer game payout structures follow standard industry configurations defined by the provider and are accessible within the game interface.

Winnings are calculated automatically by the Platform upon determination of a game outcome and credited to the player's account balance in real time. The Company does not manually intervene in payout calculations.



Section 2. Description of Periodically Used Test Methods for Quality Monitoring

1. Purpose and Scope

This section describes the quality monitoring framework applied by the Company to ensure the ongoing integrity, reliability, security, and regulatory compliance of its gaming Platform and all associated systems. Quality monitoring encompasses both internal testing conducted by the Company and external testing performed by accredited third-party laboratories in relation to game software, platform infrastructure, payment systems, and security controls.

The Chief Technology Officer ("CTO") holds primary operational responsibility for the implementation and oversight of the quality monitoring program.

2. Game Software and RNG Certification

All game titles integrated into the Platform are required to hold a valid certificate of conformity issued by an accredited independent testing laboratory prior to being made available to players. Recognised laboratories include Gaming Laboratories International (GLI), BMM Testlabs, eCOGRA, iTech Labs, and NMi Gaming. Certification confirms that the game software and its embedded Random Number Generator ("RNG") meet applicable technical standards for statistical randomness, unpredictability, and payout accuracy.

Responsibility for obtaining and maintaining game-level certifications lies with the respective third-party game provider. The Company, through its Platform partner, verifies the existence and currency of applicable certifications before any new game title is enabled on the Platform.

Where a game provider releases a material update to a game's RNG logic, payable, or payout structure, the Company verifies through the Platform that updated certification has been obtained prior to deployment of the revised version on the Platform.

On an ongoing basis, the Company monitors game-level performance data through the Platform reporting module, comparing actual observed RTP over rolling periods against the certified theoretical RTP. Sustained or unexplained deviations are escalated to the Platform and the relevant provider for investigation; where a deviation cannot be satisfactorily resolved, the affected game may be suspended pending rectification.

3. Platform Functionality Testing

Pre-deployment testing: Prior to any new software release, platform update, or integration of a new game provider or payment method, the Company independently conducts functional testing in-house, through its own technical team under the coordination of the CTO, in a staging environment that mirrors the production Platform. This testing is carried out by the Company itself, separately from any testing performed by the Platform or other third-party providers, and covers correct game loading and rendering across supported devices and browsers, accurate bet placement and payout calculation, real-time crediting of player balances, correct functioning of bonus mechanics, and integrity of all player-facing informational elements. No update is promoted to the production environment until all test cases have passed and CTO sign-off has been obtained. Where considered necessary, the Company may engage an independent third-party provider to conduct or supplement this testing.

Regression testing: Following each Platform update, regression testing is performed against a maintained baseline test case library to verify that previously functioning features have not been adversely affected by new deployments.

Performance and load testing: Periodic load testing is conducted to assess Platform stability under high concurrent user volumes. Tests simulate peak traffic conditions and measure system response times, uptime, and error rates. Results are reviewed by the CTO and any identified bottlenecks are addressed prior to anticipated traffic peaks (e.g., major promotional events or newly launched markets).

4. Security Testing

Penetration testing: The Company commissions independent penetration testing of the Platform's infrastructure and web application layer no less than once per year, and following any significant architectural change. Testing is conducted by qualified external security specialists. Findings are classified by severity, and identified vulnerabilities are remediated within defined timelines based on their risk classification. Test reports and remediation records are retained by the CTO.

Vulnerability scanning: Automated vulnerability scanning of the Platform's infrastructure is performed on a regular basis. Identified vulnerabilities are assessed, prioritised, and addressed in accordance with the Company's information security policy.

Access control review: User access rights to administrative systems, the back-office, and sensitive data repositories are reviewed quarterly by the CTO. Redundant or excessive access permissions are revoked, and access logs are reviewed for anomalous activity.

5. Payment Systems Testing

The payment processing module is subject to end-to-end functional testing prior to the activation of any new payment method or PSP integration, covering deposit and withdrawal flows, currency conversion accuracy, balance update integrity, and error handling. On an ongoing basis, transaction processing is monitored through the Platform's reporting tools for errors, failed transactions, and processing anomalies. Material issues are escalated to the relevant PSP and to the Company's finance function for resolution.

6. Incident Management and Corrective Action

All quality failures, system incidents, security events, and material deviations from expected performance identified through testing or monitoring are recorded in an incident log maintained by the CTO. Each incident is classified by severity, assigned to a responsible owner for resolution, and tracked through to closure. A root cause analysis is performed for significant incidents. Where an incident has potential regulatory implications, the CCO is notified.

Section 3. The Way of Storing Players' Personal Data and Other Details

1. Regulatory Basis

Data storage and retention practices described in this section apply in addition to, and without prejudice to, the Company's broader data protection obligations under applicable data protection legislation and the Company's internal Privacy Policy.

2. Categories of Player Data Stored

In accordance with the current guidance issued by the Government of Curaçao, the Company stores, on a weekly basis at minimum, the following categories of critical player information for each player holding an account with the Company:

2.1 Player identification. A unique, system-generated player identification code that cannot be directly traced to the player's identity by a third party but corresponds unambiguously to the player's underlying registration data, enabling secure cross-referencing without exposing personal identifiers in routine reporting datasets.

2.2 Registration and identity data. The player's account number; age and place of residence as provided at registration; and an indication of the type of identification document used during the KYC verification process (e.g., passport, national ID card, driver's licence) together with its associated document number.

2.3 Financial activity data. The total amount of deposits and withdrawals per player, recorded per calendar day.

2.4 Wagering data. The total amount of bets placed per player, recorded per calendar day.

2.5 Losses and winnings data. The total amount of losses per player per calendar day, together with winnings per calendar day, broken down into: (i) winnings paid out to the player; (ii) winnings awarded as a bonus or promotional credit; and (iii) winnings blocked due to a suspicion of fraud or an ongoing investigation.

2.6 Account balance data. The opening and closing balance of the player account per calendar day, with an indication of the amount that is freely withdrawable as distinct from amounts subject to wagering requirements, holds, or other restrictions.

3. Data Storage Infrastructure

3.1 Tier-IV data centre. The Company's general operational infrastructure, including the gaming platform, transaction processing systems, and broader player account records described in Section 4 below, runs on servers leased and operated by the Company through third-party cloud infrastructure providers (including Amazon Web Services). Players' critical data, as defined in described in Section 2 above, is separately stored on servers located within a Tier-IV certified data centre situated in Curaçao, in compliance with the applicable regulatory requirement.

3.2 Storage frequency. Critical player data is extracted from the Platform and recorded into the Company's compliance data store on a weekly basis, at minimum. Each weekly dataset reflects data aggregated per calendar day for the relevant reporting period, distinguishing the calendar date to which the data refers from the date on which the dataset is generated or submitted.

3.3 Dataset structure. Player data is maintained in structured tabular form, with each record corresponding to a unique player identification code and a specific calendar date.



The dataset includes dedicated fields for deposits, withdrawals, bets, losses, winnings (split by category), and opening/closing account balances, together with a calculated net cash-flow field and a calculated locked/restricted balance field, derived automatically from the underlying transactional data. A data dictionary documenting each field's definition, source, and calculation logic is maintained alongside the dataset and made available to the CGA upon request.

4. Storage of Other Player Account Details

In addition to the critical data described in Section 2, the Company maintains broader player account records within the Platform's player management module, including: full registration details collected at account opening; KYC/AML verification records and supporting identification documents; communication history with the player (including correspondence relating to account verification, complaints, and responsible gaming interactions); self-exclusion and limit-setting records; and complete transaction history beyond the daily aggregated figures referenced in Section 2.

These broader account records are stored on the Company's leased operational infrastructure, including third-party cloud infrastructure providers (including Amazon Web Services) underpinning the Platform, distinct from the Tier-IV facility in Curaçao, which is reserved for the critical player data required under in accordance with the laws of Curaçao and the official guidelines. Access to these broader records is governed by the Company's internal access control policy described in Section 5 below. While the weekly replication to the Tier-IV facility addresses the specific critical-data requirement under in accordance with the laws of Curaçao and the official guidelines, the Company's full player account records are retained on its operational infrastructure for the duration required under applicable AML and data protection legislation.

5. Data Security and Access Control

5.1 Encryption. Player data is encrypted both at rest and in transit, using industry-standard encryption protocols (TLS for data in transit; AES-256 or equivalent for data at rest).

5.2 Access restrictions. Access to stored player data is restricted to authorised personnel on a need-to-know basis, determined by role and function. Access rights are reviewed periodically by the CTO, in line with the access control review described in Section 2(4) of this Operations Manual.

5.3 Audit logging. All access to, and extraction of, stored player data is logged, including the identity of the accessing user, the timestamp, and the scope of data accessed. Audit logs are retained and made available for internal review and regulatory inspection.

5.4 Backup and integrity. The Tier-IV data centre maintains redundant backup systems to ensure data integrity and availability in the event of hardware failure or other technical disruption. Backup procedures are tested periodically to confirm data recoverability.

6. Data Retention

Player data described in this section is retained for the period required under applicable Curaçao gaming legislation, AML/CTF legislation, and any other applicable regulatory or tax retention requirement, and in any event for a period sufficient to allow the CGA to conduct historical inspections within its statutory powers. Upon expiry of the applicable retention period, and subject to any overriding legal obligation to retain data for a longer period, data is securely deleted or anonymised in accordance with the Company's data retention and deletion policy.

Section 4. Description of Visual Elements Shown to Players Through the Gaming Website

1. Purpose

This section describes the visual elements presented to players through the Platform's website (gravira.com), as accessed via desktop and mobile web browsers. The Platform's visual design is implemented and maintained on the Company's behalf through the Platform technology stack, in accordance with the Company's brand guidelines.

The Company also has an additional authorised domain, vashbet.com which is not currently operational. The domain carries no visual design, branding, or player-facing content, has not been developed or launched, and is not accessible to end users or used to offer games of chance in any form. The Company is currently focused exclusively on the development and operation of its authorised brand, gravira.com. Should vashbet.com be developed and launched as an active, player-facing domain in the future, this section of the Operations Manual will be updated accordingly to describe its visual elements at that time. The description below relates exclusively to the visual elements currently shown to players through gravira.com.

2. Branding and Header

The Platform is branded under the trademark "Gravira," displayed via a logo combining a stylised gold "G" icon with the wordmark "GRAVIRA" in gold/orange lettering, positioned in the top-left corner of every page. The overall colour scheme is a dark navy-blue background with gold and orange accent colours used for calls to action, highlights, and branding elements.

The main navigation header, present across the Website, includes the following primary menu items: Casino, Live Casino, Promotions (displaying a numerical badge indicating the current count of active promotions), Quests & Rewards, and Tournaments. A language selector, displaying the currently selected language together with a corresponding flag icon, is located in the top-right corner.

For unauthenticated visitors, the header displays "SIGN IN" and "SIGN UP" action buttons. For authenticated (logged-in) players, the header instead displays: a message/notifications icon; the player's current account balance with an expandable dropdown; a "DEPOSIT" call-to-action button; and a dropdown menu identifying the logged-in player by username.

3. Homepage and Game Lobby

The homepage features a rotating promotional banner (carousel), displaying time-limited welcome offers and promotions — for example, a deposit-match welcome bonus expressed as a monetary amount plus a number of free spins, accompanied by illustrative graphics (e.g., a treasure chest, gold coins) and a "SIGN UP NOW" call-to-action button. Carousel navigation arrows and position indicators allow players to browse between multiple promotional banners.

Below the banner, a horizontal category filter bar allows players to browse the game catalog by category, including: Lobby, All Games, Recommended, Hot Now, Top, New Releases, Bonus Wagering, and thematic or seasonal categories (e.g., Football Slots, Summer Slots, Classic Slots, Book Slots), each accompanied by a descriptive icon, with an expandable "More" option for additional categories. A search function is also available within this bar.

Game content is displayed in a card/tile format, organised into thematic rows (e.g., "Recommended," with a "VIEW ALL" link indicating the total number of games in that grouping). Each game tile displays



the game's promotional artwork, the game title, the name of the providing studio, and a "favourite" (star) icon allowing the player to bookmark the game for quick access.

4. Player Account Area

Authenticated players access a dedicated "Account Profile" area via the player dropdown menu or sidebar navigation. The account area sidebar displays the player's username and unique account ID, a breakdown of the player's account balance (total balance, real balance, and bonus balance, each with an accompanying information tooltip), and a vertical navigation menu providing access to: Account Profile, Bonuses, Deposits and Payouts, Responsible Gaming, History, Promo Codes, and Logout.

The Account Profile section itself is organised into tabs: Personal Details, Change Password, and Verification. The Personal Details tab displays the player's registration information — email address (with a "Verify Email" action where applicable), phone number, first and last name, date of birth (broken into day/month/year fields), country, city, address, and postal/zip code. Fields containing identity-verified data are displayed with a lock icon, indicating that the relevant information cannot be amended by the player directly once verified, in support of the integrity of the Company's KYC records. A "SAVE" action is provided to confirm any permitted changes.

5. Footer and Regulatory Disclosures

The footer, present on all pages, is organised into the following sections:

5.1 Game providers. A "PROVIDERS" panel displays the logos of integrated game studios in a paginated grid (navigable via arrow controls), providing players with visibility into the range of content providers available on the Platform.

5.2 Informational and policy links. An "INFORMATION" column provides direct links to the Platform's Responsible Gaming Policy, Privacy Policy, KYC Policy, Terms and Conditions, AML/CTF Policy, About Us page, and Player Complaints Policy, among others.

5.3 Licence disclosure. A "LICENSE" panel displays the Company's full regulatory disclosure, confirming that the Platform is owned and operated by Horizonix Corp N.V., stating the Company's registration number, confirming that the Company is licensed by the Curaçao Gaming Authority under the applicable licence number issued pursuant to the National Ordinance on Games of Chance, and providing the Company's registered address. The panel also references the verifiability of the licence via the regulator's digital seal.

5.4 Responsible gaming and certification badges. Adjacent to the licence disclosure, the footer displays a row of trust and responsible-gaming badges, including an "18+" age-restriction indicator and logos associated with responsible gambling support organisations (e.g., GamCare, Responsible Gambling, Gamblers Anonymous) and the Curaçao Gaming Authority's certification mark.

5.5 Payment methods. A "PAYMENT METHODS" panel displays the logos of all accepted deposit and withdrawal methods, including card schemes (Visa, Mastercard), regional payment systems (e.g., Interac), and a range of supported cryptocurrencies (e.g., Bitcoin, Litecoin, Tron, and stablecoins), giving players visibility into available transaction options before initiating registration or deposit.

5.6 Social media and utility controls. The footer additionally provides links to the Company's social media and messaging channels (e.g., WhatsApp, X, YouTube, Facebook, Telegram), a language selector, and a "scroll to top" control.



Section 5. Description of Technical Measures Put in Place to Prevent the Admission of Banned Natural Persons

1. Purpose and Regulatory Basis

This section describes the technical measures implemented by the Company to prevent natural persons who are banned from playing games of chance under the National Ordinance, including persons subject to a self-exclusion, persons on a national or group-wide exclusion register, minors, and persons otherwise legally prohibited from participating, from accessing or playing the games of chance offered through the Websites.

The Compliance Officer ("CCO") holds primary operational responsibility for the design, implementation, and ongoing supervision of the exclusion-control framework described in this section, supported by the Company's integrated third-party verification providers.

2. Categories of Banned and Excluded Persons

The technical measures described in this section are designed to prevent access by the following categories of persons:

2.1 Minors. Natural persons under the age of 18 (or such higher minimum age as may apply under the law of the player's jurisdiction of residence), who are prohibited from registering an account or playing under any circumstances.

2.2 Self-excluded players. Players who have voluntarily applied a self-exclusion to their own account through the Platform's responsible gaming tools, for the duration of the applicable exclusion period.

2.3 Group-wide excluded persons. Persons registered on any applicable national self-exclusion or gaming exclusion register recognized under the National Ordinance, as well as persons excluded by the Company on a precautionary or risk basis (e.g., following a finding of fraud, manipulation, or breach of the Company's terms).

2.4 Persons subject to sanctions or AML restrictions. Natural persons appearing on applicable sanctions, PEP, or adverse media watchlists, whose participation would expose the Company to AML/CTF or sanctions compliance risk.

2.5 Persons in restricted jurisdictions. Natural persons located in, or resident of, jurisdictions in which the Company does not hold the requisite authorisation to offer games of chance, or which are subject to a geo-blocking restriction under the Company's licensing conditions.

3. Technical Measures at Registration Stage

3.1 Age verification. At the point of registration, players are required to declare their date of birth, which is automatically validated by the platform against the applicable minimum age threshold. Accounts failing this initial check are blocked from completing registration.

3.2 Identity verification (KYC). Identity verification is performed via reputable third-party compliance service providers integrated with the Platform. These providers conduct document verification (validating the authenticity of the identification document submitted at registration), biometric or facial-match verification where applicable, and database cross-checks confirming the identity, age, and stated place of residence of the registering player. The third parties providers facilitate the verification

workflow and enforces the resulting outcome (approval, rejection, restriction, or escalation for manual review), while the underlying verification and screening services are delivered by the external providers under the Company's oversight.

3.3 Sanctions, PEP, and watchlist screening. As part of the onboarding process, each new player is automatically screened against applicable international sanctions lists, politically exposed persons ("PEP") databases, and adverse media sources via the Company's integrated compliance service providers. A positive match triggers an automated hold on the account pending manual review by the CCO or designated compliance personnel.

3.4 Geolocation and IP-based restriction. The Platform applies real-time geolocation verification, using a combination of IP address detection and, where applicable, device-level location data, to determine the player's actual location at the point of registration and at subsequent login and play sessions. Players detected in a restricted jurisdiction are automatically blocked from completing registration or accessing real-money games of chance, irrespective of the country declared during registration.

3.5 Device and account fingerprinting. The Platform applies device fingerprinting technology to detect attempts by a previously excluded or banned player to circumvent an exclusion by creating a new account. Indicators include matching device identifiers, IP address patterns, payment method details, and other behavioural or technical markers associated with a known excluded account. Matches are automatically flagged for compliance review and the new account is suspended pending investigation.

4. Technical Measures During Ongoing Account Activity

4.1 Real-time exclusion enforcement. Where a player applies a self-exclusion, or is placed on an exclusion list by the Company or identified on a national exclusion register, the Platform immediately and automatically suspends the player's ability to log in, deposit funds, or place wagers, for the duration of the applicable exclusion period. Reversal of a self-exclusion prior to expiry of the minimum statutory or platform-defined cooling-off period is technically prevented by the system.

4.2 Exclusion register readiness. Where the CGA or Curaçao authorities introduce or recognise a national exclusion register or other mandatory exclusion database, the Company must integrate that database into onboarding and ongoing monitoring as soon as technically and legally available, and document interim manual controls until automation is completed.

4.2 Ongoing watchlist monitoring. Player records are subject to periodic re-screening against sanctions, PEP, and exclusion list updates, ensuring that a player who becomes subject to an exclusion or sanction after registration is identified and actioned in a timely manner. A positive match during ongoing monitoring triggers an automated account restriction pending compliance review.

4.3 Session-level geolocation re-verification. Geolocation verification is re-applied at login and at defined intervals during active play sessions, preventing a player from continuing to access the Website's real-money games of chance if their detected location subsequently falls within a restricted jurisdiction.

4.4 Multi-account and circumvention detection. The Company continuously monitors for indicators of attempted circumvention of an active exclusion or ban, including the creation of duplicate or linked accounts, use of VPN or proxy services to mask location, and use of payment instruments previously associated with an excluded account. Detected circumvention attempts are automatically flagged, the relevant account(s) suspended, and the matter escalated to the CCO for investigation and, where appropriate, reporting.

4.5 Responsible gaming integration. Technical exclusion controls operate in conjunction with the Company's broader responsible gaming tools (deposit, loss, and wagering limits; time-out and cooling-off periods; reality checks), ensuring that a player who has triggered a responsible-gaming-related restriction is subject to consistent enforcement across all access points and game categories.

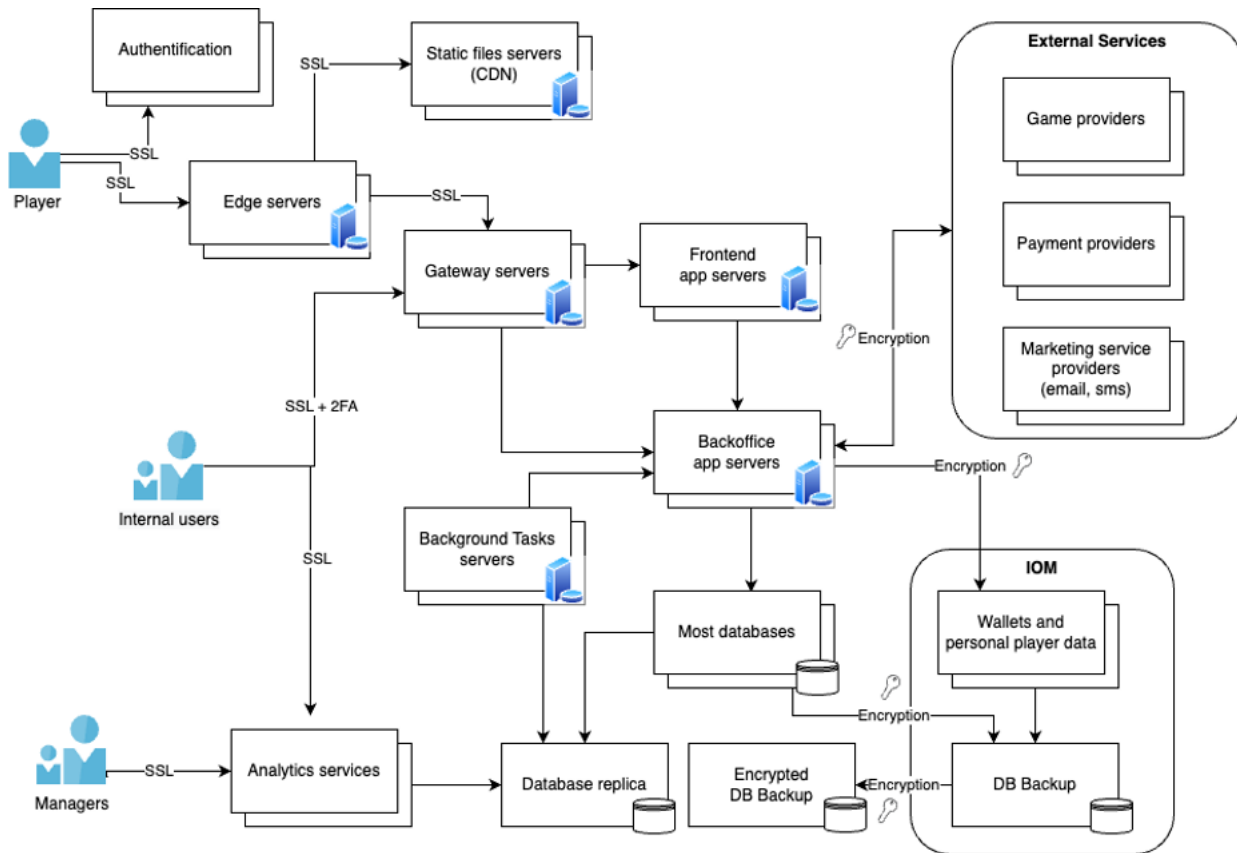
5. System Architecture and Oversight

The exclusion-control framework operates as an integrated function within the Platform player management module, drawing on real-time data feeds from the Company's third-party KYC/AML and screening providers, geolocation services, and internal exclusion records maintained by the Company. All restriction and exclusion events are logged automatically, including the trigger, timestamp, and resulting account action, and are retained for audit and regulatory inspection purposes.

The CCO maintains oversight of the exclusion-control framework, including periodic review of its effectiveness, investigation of flagged matches and circumvention attempts, and escalation of confirmed breaches in accordance with the Company's AML/CTF and responsible gaming policies. Any incident involving a confirmed instance of a banned or excluded person accessing the Website is recorded as a compliance incident in accordance with the incident management process described in this Operations Manual, and is assessed for any required notification to the CGA.

Section 6. Diagram of the Technical Infrastructure and Description of Restoration Possibilities

1. Technical Infrastructure Diagram



The Company's technical infrastructure is organized into the following layers:

- Access layer.** Players connect via SSL to dedicated Edge servers, with a separate Authentication module also accessed via SSL. Static assets are served from Static Files servers (CDN), also reached via SSL. Internal users and managers access the system separately: internal users connect to Gateway servers via SSL with two-factor authentication ("SSL + 2FA"), while managers access reporting exclusively through dedicated Analytics services via SSL.
- Application layer.** Edge servers route player traffic via SSL to Gateway servers, which in turn route to Frontend application servers (serving the player-facing platform) and to Backoffice application servers (supporting internal operations, reporting, and administrative functions). Background Tasks servers handle asynchronous processing and connect directly to the core database layer.
- Data layer.** The core operational data is held in the primary database cluster ("Most databases"), with a Database replica maintained for read access and resilience, and an Encrypted DB Backup maintained as a further safeguard. Player wallets and personal player data are held in a separate, isolated module ("IOM"), encrypted and segregated from the general application databases, with its own dedicated DB Backup, which is in turn encrypted.
- External integrations.** The Backoffice application servers connect, via encrypted channels, to External Services, comprising Game providers, Payment providers, and Marketing service providers (email/SMS), enabling game content delivery, payment processing, and player communications respectively.

- e) Encryption. All connections to external services, to the IOM (wallets and personal data), and to backup systems are encrypted, in addition to the SSL protection applied across all access-layer connections.

2. Restoration Possibilities in the Event of a Technical Emergency

2.1 Database redundancy. The Database replica provides a live, redundant copy of the core operational database, enabling rapid failover and continued data availability in the event the primary database becomes unavailable, with minimal disruption to platform operations.

2.2 Encrypted backups. Both the core database and the IOM (wallets and personal player data) are backed up separately into dedicated, encrypted backup stores (Encrypted DB Backup and DB Backup, respectively). This separation ensures that, in the event of a failure or compromise affecting either the general operational data or the sensitive player/wallet data, the unaffected dataset and its backup remain intact, and the affected dataset can be restored from its corresponding encrypted backup.

2.3 Isolation of sensitive data. Because wallets and personal player data are held in a segregated module (IOM) with its own independent backup chain, a technical incident affecting the general application or database layer does not, by design, compromise the integrity or availability of player funds and personal data, and vice versa.

2.4 Restoration procedure. In the event of a technical emergency (e.g., hardware failure, database corruption, or service outage), the Company's technical team, under the supervision of the CTO, restores affected systems by: (i) failing over to the Database replica to maintain continuity of core services; (ii) restoring affected data from the most recent Encrypted DB Backup or DB Backup, as applicable; and (iii) verifying data integrity and consistency before resuming full production operations. Recovery actions are logged and reviewed as part of the Company's incident management process described in this Operations Manual.

2.5 Service continuity. Because the access layer (Edge servers, Gateway servers, Authentication, CDN) is structurally separated from the application and data layers, partial outages can frequently be isolated and addressed without a full platform shutdown, limiting player-facing disruption during restoration.



Section 7. Description of How the Principles of Responsible Gaming Have Been Implemented in the Operation

1. Purpose and Regulatory Basis

This section describes how the Company has implemented the principles of responsible gaming within its operations, in accordance with the Company's Responsible Gaming Policy and the relevant provisions of the LOK.

The Company's Responsible Gaming Policy, maintained as a standalone governing document and published on the Website, sets out the detailed rules and procedures summarized in this section. Where any discrepancy arises between this summary and the full Responsible Gaming Policy, the full Policy governs.

Oversight and execution of the Company's responsible gaming framework is assigned to the Compliance Officer who is responsible for the design, implementation, and ongoing supervision of all responsible gaming measures described below.

2. Prevention of Participation by Vulnerable Persons

In accordance with Article 2.2, third paragraph, and Article 1.4(e) of the LOK, the Company does not knowingly give a person who can reasonably be assumed to be a vulnerable person, including minors, persons lacking sufficient control over their gambling behavior, persons who have been excluded from gambling (voluntarily or compulsorily), and persons declared bankrupt by a competent court — the opportunity to play games of chance.

2.1. Age verification. At registration, players must declare their date of birth and confirm, via a mandatory checkbox, that they are eighteen years of age or older. Self-attestation alone is not relied upon: the Company applies additional KYC verification, including submission of a valid government-issued identity document prior to first withdrawal or upon reaching applicable thresholds, supplemented at the Company's discretion by electronic identity checks, payment method validation, third-party database verification, and biometric verification. Should the Company become aware that a registered player is a minor, the account is closed immediately, applicable civil law consequences are assessed (including refund of deposits and forfeiture of winnings, where applicable), and the player is formally notified of the closure and its reason.

2.1. Behaviour-based identification of vulnerable persons. The Company actively monitors player activity to identify indicators consistent with vulnerability or problem gambling, including: sudden unexplained increases in deposit or wagering frequency; repeated failed transactions due to insufficient funds; repeated reversal of withdrawal requests; inexplicably extended play sessions; disproportionate increases in contact with customer support, including agitated requests for bonuses; frequent changes to responsible gaming settings; and attempts to open multiple accounts to circumvent limits or exclusions. Monitoring is performed both by frontline staff (customer service and VIP management) and by automated platform tools. No single indicator is treated as determinative; a finding of risk is generally based on the presence of multiple, consistent indicators. All responsible gaming interactions, whether player- or operator-initiated, are recorded in the player account management system together with the relevant indicators and resulting actions.

2.3. Intervention. Players identified as at-risk are informed of the available responsible gaming tools (deposit limits, cooling-off, self-exclusion). Where appropriate, the Company applies an escalation protocol that may include mandatory deposit limits, temporary account suspension pending assessment, or permanent exclusion in cases of severe or persistent risk. Responsible gaming measures are never used as a pretext to delay or prevent legitimate player withdrawals; any such misuse is treated as a breach of the Company's licence conditions.

3. Self-Exclusion and Cooling-Off

The Company provides players with two distinct, player-controlled mechanisms for managing their own gambling activity, accessible at all times via the Responsible Gaming Section of the Website:

3.1 Cooling-off. A short-term, temporary restriction on gambling activity, available in durations of 24 hours, 7 days, 1 month, or 3 months. Players may elect the scope of the restriction (brand, vertical) in addition to the mandatory duration and marketing opt-out elements. During a cooling-off period, deposits and gameplay are blocked, withdrawals remain available, and the player's account is not closed. Restrictions take effect immediately upon player selection; the Company does not question the player's decision, offer bonuses or promotions to discourage the restriction, or delay activation. Accounts are reactivated automatically upon expiry of the selected period.

3.2 Self-exclusion. A long-term restriction from all gambling activity across all of the Company's brands and verticals, available for a minimum statutory period of one year, with extended options of 3, 5, or 10 years, or lifetime, in compliance with Article 5.4(2) of the LOK. Self-exclusion can be initiated and completed entirely online by the player, without requiring email communication or Company approval, and takes effect immediately. Upon activation, the player's account is closed, marketing communications are automatically blocked, and the Company applies reasonable measures to detect and prevent the creation of duplicate accounts by the excluded individual, including blocking known payment methods associated with the excluded account. Reactivation following expiry of the self-exclusion period requires an affirmative written request from the player; the Company does not initiate re-engagement with a self-excluded player.

3.3 Neutral process design. Consistent with the Company's Responsible Gaming Policy, players are not guided or influenced toward one option over the other, and no incentives, reassurances, or bonus offers are presented during either process. Players self-identifying as vulnerable are offered the option to proceed directly to self-exclusion.

3.4 Operator-initiated exclusion. Independently of player-initiated restrictions, the Company may exclude a player as a high-risk intervention measure where the player displays problematic gambling behaviour or engages in attempted or actual criminal activity through the Website. The Company does not exclude players solely on the basis of the size of their winnings. Operator-initiated exclusions are formally documented and records are retained for no less than five years.

4. Player Information, Tools, and Self-Assessment

A dedicated, clearly identifiable Responsible Gaming Section is maintained on the Platform at all times, providing players with accessible information to support informed decision-making, direct access to all available responsible gaming tools (limit-setting, cooling-off, self-exclusion), and contact details for raising responsible gaming concerns via email or live chat. The Responsible Gaming Section is also incorporated into the Company's Terms and Conditions, accessible within one click of the homepage, and made available in English (the governing version in case of discrepancy), with additional languages provided at the Company's discretion to reflect target markets.

Players have access to a record of their betting and wagering history, including transaction timestamps, covering at least the preceding six months, with longer periods available on request within the applicable regulatory timeframe. Players are encouraged to periodically assess their own gambling behavior using self-assessment resources referenced within the Responsible Gaming Section, including the Gamblers Anonymous twenty-question self-assessment and a short-form screening tool addressing cutting down, annoyance at criticism, guilt, and "eye-opener" gambling behaviour, together with signposting to external support organizations (GamCare, Gambling Therapy, Gamblers Anonymous, BeGambleAware, and GamBlock).

The Company further provides deposit limit functionality, enabling players to set daily, weekly, or monthly deposit limits. Requests to tighten a limit take effect immediately; requests to loosen a limit are subject to a mandatory 24-hour cooling period before implementation, consistent with the Company's policy of not facilitating unconsidered increases in gambling exposure.

5. Staff Training

In accordance with the Company's Responsible Gaming Policy, customer service and responsible gaming personnel receive training covering the recognition of signs of gambling-related distress (including agitation, aggression, or financial desperation), the conduct of sensitive and structured conversations with at-risk players, and the appropriate referral of players to relevant support resources and responsible gaming tools.

6. Consumer Advertising and Marketing

The Company's marketing, promotional, and advertising activity is conducted in accordance with the following principles: marketing does not target vulnerable persons; gambling is not portrayed as a means of achieving financial success or resolving financial difficulty; advertising does not misrepresent the role of skill in games of chance that are determined purely by chance; gambling is not portrayed as a substitute for emotional or mental well-being; marketing materials do not feature minors or depict minors engaging with gambling content; advertising contains no explicit or sexual content; and gambling is not linked, in messaging, to smoking, drug use, alcohol consumption, or related harmful behaviors.

Bonuses and promotions are communicated transparently with clear terms and conditions, and are not used to encourage excessive gambling. The Company remains responsible for materials provided to affiliates, sponsors, brand ambassadors, and social media influencers engaged on a paid basis, and requires all such third parties to adhere to the Company's Responsible Gaming Policy. All advertising includes a clearly visible responsible gaming message.

7. Enhanced Measures

Where warranted by the Company's risk profile or player base, the Company may apply enhanced responsible gaming measures, including signposting to third-party device- and network-level gambling-blocking tools (e.g., BetBlocker, GamBlock, Gamban); automated or manual pop-up interventions linking the player to a responsible gaming professional in response to concerning behaviour; additional limit types (loss limits, time limits, wager limits) where appropriate to the target market; and reality-check functionality, such as a persistent, real-time session timer, periodic session-duration prompts, and player-configurable reality check alerts requiring active player confirmation before play may continue.



Section 8. The Most Recent Text of the General Terms and Conditions Used by the Operation

1. Purpose

This section confirms the most recent version of the General Terms and Conditions applied by the Company in respect of its operation of the Website.

2. General Terms and Conditions

The current, applicable version of the Company's General Terms and Conditions, governing the relationship between the Company and its registered players, is attached as Annex 1 to this Operations Manual.

The General Terms and Conditions are also published and kept continuously accessible to players on the Websites, in accordance with the Company's transparency obligations under the LOK. The version published on the Website at any given time is the version in force, and corresponds to the version maintained in Annex 1.

3. Version Control

The Company maintains version control over its General Terms and Conditions. Each update is duly dated, and new versions are retained in the Company's internal records for audit purposes. When the General Terms and Conditions are updated, the Company accordingly adds the current versions of Annex 1 to this Operations Manual. Previous versions cease to have effect and are marked accordingly. Where necessary, the Company also makes amendments to this Operations Manual. In addition, where required by applicable law, the CGA is duly notified of the updated versions, which are provided to the CGA for review in accordance with the applicable regulatory requirements.

4. Cross-References

The General Terms and Conditions incorporate, by reference or in substance, the Company's Responsible Gaming Policy, Privacy Policy, KYC Policy, AML/CTF Policy, and Player Complaints Policy, each of which is separately maintained and referenced elsewhere in this Operations Manual.

Annex 1: General Terms and Conditions of Horizonix Corp N.V. (gravira.com) — [most recent version to be attached].

Section 9. Description of How the Licensee Settles Disputes with Players

1. Purpose and Regulatory Basis

This section describes the procedure applied by the Company for settling disputes with players, in accordance with Article 5.3 of the LOK and the Company's standalone Player Complaints Policy, published and continuously accessible at the Website. Where any discrepancy arises between this summary and the full Player Complaints Policy, the full Policy governs.

2. Eligibility and Submission

Only registered players on the Websites may submit a complaint. Complaints must be submitted free of charge within six (6) months of the incident giving rise to the complaint or, for peer-to-peer gaming or ante-post fixed-odds betting, within six months of the conclusion of the relevant event. Prompt submission is advised for in-running sports betting complaints, given the potential unavailability of underlying data over time. In accordance with Article 1.3(c) of the LOK, a player's claim cannot be sold, donated, rented, leased, pawned, or pledged to a third party.

Complaints are submitted using the Company's standard Player Complaint Submission Form, available for download in Word and PDF format on the Website, and sent by email to complaints@gravira.com together with any supporting documentation (e.g., screenshots, transaction records, chat transcripts, game IDs, or payment confirmations). Complaints may be submitted in English, Dutch, or Papiamentu for official review; complaints submitted in other languages may require translation before processing. The complaint form requires the player to identify, among other details, the relevant complaint category — covering matters such as deposit and withdrawal issues, bonus terms, account restrictions, alleged errors or unfairness in game outcomes, responsible gaming concerns, treatment of player balances, KYC/verification, data protection, technical issues, AML concerns, and licence or regulatory matters.

Responsible gaming complaints and complex complaints must be reviewed by human staff. AI tools, if used, may only support administrative triage, drafting, categorisation, or consistency checks, and all complaint outcomes must remain subject to human supervision.

The Company's internal complaint-handling process is entirely free of charge to the player, with no administrative, handling, review, communication, or case-management fees applied at any stage.

3. Acknowledgement and Resolution Timelines

Upon receipt of a complaint, the Company confirms receipt in writing within one (1) week (or within two business days for complaints relating to responsible gaming), explains how the complaint will be processed, and provides an expected resolution timeline.

Responsible gaming complaints are prioritised, with the Company using best efforts to resolve such complaints within five business days. All other complaints are assessed and responded to within four weeks of submission, extendable once by a further four weeks where necessary, subject to prior written notice to the player explaining the reason for the extension.

4. Internal Resolution Outcome

Following assessment, the Company communicates its determination to the player in writing, setting out the outcome of the complaint and, where applicable, any remedial action taken (e.g., correction of

an account or transaction error, release of a previously held balance, reinstatement of access, or other appropriate redress). Where a complaint is not upheld, the Company provides the player with a reasoned explanation of its decision and informs the player of the further escalation options described below.

5. Escalation to Alternative Dispute Resolution (ADR)

Where a complaint is not resolved to the player's satisfaction through the Company's internal complaint procedure, and the Company's internal process has first been fully exhausted, the player may escalate the matter to an independent, CGA-approved Alternative Dispute Resolution ("ADR") provider, at no cost to the player, with the Company bearing the costs of the ADR process.

The Company has concluded an ADR agreement with CADRE B.V., a CGA-approved, certified, and authorised ADR provider (certificate number CGA/ADR/2025/01, effective from 9 February 2026 to 9 February 2029), registered at 39 Scharlooweg, Willemstad, Curaçao (company registration number 165229). Players wishing to escalate a dispute to CADRE must do so via CADRE's official claim form, accessible at <https://cadre.online/file-a-claim-international/>, in accordance with CADRE's published rules of procedure (<https://cadre.online/rules-of-procedure/>), unless CADRE expressly instructs otherwise. General enquiries may be directed to CADRE at operators@cadre.online.

A minimum claim value of EUR 5,000 applies for a dispute to be eligible for ADR escalation, save that this minimum threshold does not apply to complaints concerning responsible gaming.

6. Reporting to the CGA

The CGA does not mediate or determine individual player disputes. Where a player reasonably believes that the Company has breached an applicable regulatory requirement, the player may report the matter directly to the CGA via the official complaint form available on the CGA's website. The Company maintains records of all player complaints, which may be requested, accessed, reviewed, or inspected by the CGA at any time as part of its supervisory, monitoring, investigative, or enforcement functions.

7. Record-Keeping

The Company maintains a complete record of each complaint received, including the complaint category, supporting documentation, internal correspondence, the outcome reached, and any escalation to ADR, for the retention period required under applicable regulatory requirements. These records are made available to the CGA upon request and support the Company's periodic review of complaint trends as part of its broader compliance monitoring framework.

Section 10: The Digital Records Kept of Specific Critical Information About Players, Their Gaming Transactions, and Their Financial Transactions

1. Purpose and Regulatory Basis

This section describes the digital records maintained by the Company regarding specific critical information about players, their gaming transactions, and their financial transactions, in accordance with Article 5.9 of the National Ordinance on Games of Chance and the underlying data storage requirements. This section should be read together with Section 3 of this Operations Manual, which describes the Company's broader data storage architecture; this section focuses specifically on the nature of the records kept and their continuous availability to the CGA.

2. Scope of Records Maintained

The Company maintains digital records of the following critical information for each player holding an account with the Company:

2.1 Player identification records. A unique, system-generated player identification code that cannot be directly traced to the player's identity but corresponds unambiguously to the player's underlying registration data.

2.2 Player account and identity records. The player's account number, age and place of residence as provided at registration, and an indication of the type and number of the identification document used at registration.

2.3 Financial transaction records. The total amount of deposits and withdrawals per player, recorded per calendar day.

2.4 Gaming transaction records. The total amount of bets placed per player, recorded per calendar day.

2.5 Outcome records. The total amount of losses per player per calendar day, together with winnings per calendar day, broken down into winnings paid out, winnings awarded as bonus or promotional credit, and winnings blocked due to suspected fraud or an ongoing investigation.

2.6 Account balance records. The opening and closing balance of each player account per calendar day, with an indication of the freely withdrawable amount.

3. Storage Location and Availability to the CGA

The records listed in Section 2 above are stored on a server located within a Tier-IV certified data centre registered in Curaçao, separately from the Company's general operational infrastructure. This dataset is updated and replicated to the Tier-IV facility no less than once per week, in accordance with Article 2, and is maintained in a structured, queryable digital format, accompanied by a data dictionary describing each field's definition and source.

The records held on the Tier-IV server are kept available to the CGA at all times. The Company is able to produce the dataset, or any subset thereof requested by the CGA, within the timeframe required for inspection, in accordance with Article 5.9, third paragraph of the LOK.

4. Data Integrity and Access

Access to the digital records held on the Tier-IV server is restricted to authorised personnel on a need-to-know basis, with all access logged in accordance with the access control framework described in the relevant Sections of this Operations Manual. The integrity of the records is safeguarded through

encryption at rest and in transit, redundant infrastructure at the Tier-IV facility, and periodic verification that the weekly replication process has completed successfully and without data loss.

5. Retention

The digital records described in this section are retained for the period required under applicable Curaçao gaming legislation, AML/CTF legislation, and any other applicable regulatory or tax retention requirement, consistent with the retention principles set out in Section 3 of this Operations Manual.

Signed

A stylized handwritten signature in black ink, consisting of a series of loops and a long horizontal stroke extending to the right.

Director: Ecorpp Management N.V.