

Operational Manual

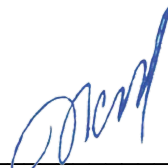
Product industry	Online Gaming
Regulator	CGA (Curacao Gaming Authority)
Operator	Lotostorm B.V.
Approved as of:	Waaigat Directors B.V.
Version No.:	v.1
Adoption Date:	18 June 2026



Rudsel Lucas o.b.o
Dempel Directors B.V.
Managing Director



Rudsel Lucas o.b.o
Waaigat Directors B.V.
Managing Director



Volodymyr Zhukovskyi
Managing Director

REGULATORY BASIS

The Operator maintains this Operational Manual in discharge of the obligation imposed by Article 5.9, first paragraph, of the National Ordinance on Games of Chance (Curaçao). Under that provision, every holder of a licence granted pursuant to Article 5.1, first paragraph, is required to keep in place at all times an operational manual that documents the manner and extent of the Operator's compliance with the National Ordinance and with the conditions and restrictions to which the Gaming Licence is subject.

1. OVERVIEW OF GAMES OF CHANCE: OFFERINGS, WAGERING FRAMEWORK, PAYMENT OPTIONS, PAYOUT PRACTICES, SOFTWARE SYSTEMS, AND RESULT GENERATION

The Operator makes available, within the bounds of its licensed authorisation, a diverse and varied portfolio of Games of Chance. The following section describes the game types on offer, the rules governing player participation, deposit and withdrawal arrangements, applicable wagering parameters, the methodology for determining and paying out prizes, the technical infrastructure supporting gameplay, and the systems by which results are generated.

1.1. Game Offering and Mechanics

The Operator's portfolio covers a range of games whose outcomes are determined by chance. Each title is developed and maintained in compliance with recognised international technical specifications and applicable regulatory standards.

Slot Games

Players interact with digital reel-based games, each presenting a unique arrangement of symbols and a defined payline structure. An individual payable accompanies each slot, setting out the qualifying combinations for prizes, the operation of any bonus mechanics, and the rules governing multipliers. Every spin result is generated independently by a certified Random Number Generator (wRNG), so that no outcome can be derived from or predicted on the basis of any previous result.

Blackjack

This card game pits players against the dealer in a contest to assemble a hand as close to a value of twenty-one as possible without going over. Players select from a range of actions—including hit, stand, double down, or split—based on their hand and the dealer's exposed card. The dealer operates according to fixed rules, ordinarily drawing on any hand of sixteen or less and standing on seventeen or above. The order in which cards are dealt is determined by a digitally randomised process underpinned by RNG technology, reproducing the unpredictability of a physical shuffle.

Roulette

Participants wager on the outcome of a ball spun around a wheel, specifically the numbered segment in which it will eventually come to rest. Both the European format (single zero) and the American format (double zero) may be available. The platform supports a range of wager types, including straight-up, split, and even-money bets. The landing position of the ball is computationally determined through RNG mechanisms, ensuring that each round produces a statistically independent and unpredictable result.

Video Poker

At the start of each round, five cards are randomly dealt to the player, who then decides which to retain and which to exchange, with the aim of completing the strongest hand possible according to standard poker rankings. Both the initial deal and any subsequently drawn cards are governed by RNG logic, ensuring consistency, integrity, and impartiality across every hand.

Live Casino Games

Live-format tables provide players with an experience that closely mirrors a physical casino environment, delivered through real-time streaming by trained and professional human dealers. All games follow established rules of play, and users may engage with the dealer in the course of each session. Unlike RNG-based products, the outcomes of live games are the product of tangible physical events—such as a card being turned or a wheel being spun—which are filmed and relayed directly to the player’s device.

1.2. RNG Systems

The outcomes of all virtual game rounds are governed by Random Number Generator (RNG) systems deployed across all of the Operator’s game providers. These systems serve the following purposes:

- to produce the result of each individual game round;
- to generate random numbers by means of mathematical algorithms or hardware-based entropy sources;
- to guarantee objectivity, so that no result is adapted or weighted in favour of either the player or the platform.

Random Number Generator (RNG) systems in operation across the platform:

a) Apply methods recognised by the industry to guarantee that all produced results are entirely random	b) Are seeded with securely generated, non-deterministic values that preclude the possibility of prediction	c) Are subject to periodic independent assessments to confirm continued compliance and to verify the integrity of randomness over time
--	---	--

1.3. Sports Betting Options

The Operator’s platform enables users to place wagers on live sporting events as well as on scheduled future matches and e-sports competitions. The following wagering types are offered:

- **Single Bets:** A wager on a single designated outcome. Winnings are calculated by multiplying the stake by the applicable odds.
- **Accumulator Bets:** A combined stake across multiple independent selections. Any losing selection cancels the entire wager. The odds applicable to each selection are multiplied together to determine the total return. Correlated outcomes are not accepted and are excluded automatically.
- **System Bets:** Constructed from multiple sub-accumulator combinations produced from a given pool of selections, covering up to 20 selections and 184,756 possible outcome combinations.
- **Chain Bets:** A succession of individual bets in which the winnings from each successful bet are rolled forward as the stake for the next. Bets are settled in the sequence shown on the slip, and the chain terminates once the available balance runs out.

- **Advance Bets:** Offered on the basis of anticipated winnings from open bets expected to settle within forty-eight hours. Open bets must be of sufficient value to cover the Advancebet amount; funds deposited after the advance has been granted cannot be applied to repayment.
- **Multibets:** A hybrid format combining single bets and accumulators. If a designated “Lobby” selection is present, it must succeed for the wager as a whole to stand; if none is designated, the bet is handled as a system bet.
- **Conditional Bets:** Structured so that each successive stake is dependent on the return from the preceding selection. If any selection is lost and no funds remain, the bet is finalised.
- **Anti-Accumulators:** A wager that pays out if any one leg of an accumulator is unsuccessful. All selections must be independent, and the calculation relies on inverse probabilities.
- **Lucky Bets:** Incorporating all possible single bets and accumulator combinations across two to eight selections, with a return achievable from even a single correct pick.
- **Patent Bets:** Covering every accumulator combination across three to eight selections, requiring a minimum of two correct picks to generate a winning accumulator.

1.4. Payment Infrastructure

Every financial transaction conducted on the platform is routed exclusively through regulated Payment Service Providers (PSPs). An extensive range of deposit and withdrawal methods—spanning both global and regional channels—is made available under the terms of formal merchant service agreements.

The following principles apply to all monetary transactions conducted on the platform:

- The Operator verifies the identity of customers before processing transactions and discharges its applicable due diligence obligations at all times.
- Withdrawals are available on a continuous basis and may be requested at any hour.
- Funds received by way of electronic payment may not be withdrawn in cash.
- Withdrawal amounts must bear a reasonable and demonstrable relationship to genuine wagering activity. Total bets placed must be at least equal to the deposit amount at minimum odds of 1.1; low-risk strategies involving opposing outcomes are disregarded for this purpose.
- Where an account presents indicators of concern, the Operator may suspend withdrawal processing pending a compliance review.
- Withdrawals must use the same payment channel as the corresponding deposit; where deposits were made through more than one method, the withdrawal is distributed across those methods in proportion.
- Transactions may only be executed using payment instruments held in the registered account holder’s name.

2. PERIODIC TESTING AND VALIDATION OF RANDOM NUMBER GENERATORS: METHODS, STANDARDS, AND CERTIFICATION FRAMEWORK

The Operator’s virtual gaming products depend for their fairness on the proper and verifiable functioning of Random Number Generator (RNG) systems. This section sets out why ongoing RNG quality oversight is necessary, what compliance benchmarks apply, what statistical methods are used to assess outputs, and how independent third-party audits are conducted on a recurring basis.

2.1. Objective of RNG Quality Monitoring

As the foundational mechanism for producing fair and unpredictable outcomes in virtual games, the RNG must satisfy rigorous technical criteria. Each RNG deployed across the platform is required to demonstrate the following:

a) Verifiable statistical randomness and an even distribution of results across all outputs	b) Effective resistance to any attempt at manipulation, exploitation, or advance prediction	c) Sustained conformity with the technical and regulatory standards applicable in recognised licensed gaming jurisdictions
---	---	--

2.2. Technical and Regulatory Compliance

All RNG systems are required to conform to the globally accepted technical frameworks governing random number generation in licensed gaming environments. The applicable compliance requirements comprise the following:

Cryptographic Integrity	Seed Security	Auditability and Documentation
Outputs must be derived from algorithms with demonstrably strong entropy properties, or from hardware-based randomness sources where applicable	Initialisation seed values must be non-deterministic and produced through secure processes, so as to eliminate any prospect of the sequence being predicted or reproduced	The complete logic underlying the generation process, the system architecture, and all relevant operational parameters must be documented in full and available for independent inspection

2.3. Statistical Testing Procedures

RNG performance is verified through a systematic programme of statistical analysis applied to the systems' outputs, which may include the following tests:

Frequency Distribution Analysis	Confirms that each possible output value is generated at a rate consistent with uniform probability, demonstrating that no values are systematically favoured or suppressed
Runs Test	Screens the output stream for atypical clustering or unexpectedly repetitive sequences that could indicate the presence of underlying bias or patterning
Autocorrelation Evaluation	Examines whether any statistical relationship exists between successive output values; the presence of such a relationship would constitute evidence of non-randomness
Chi-Square Goodness-of-Fit Test	Measures the degree to which the observed distribution of outputs aligns with the expected theoretical distribution under a uniform probability model

Entropy Analysis	Quantifies the unpredictability of the output sequence; higher entropy values correspond to a stronger degree of randomness and a lower susceptibility to prediction or exploitation
-------------------------	--

2.4. Third-Party Certification and Oversight

No RNG may be deployed within the Operator's production environment until it has been independently audited and certified by an internationally recognised testing laboratory. The certification process may encompass:

a) A detailed review of the algorithm at source code level	b) Statistical examination of a representative body of output samples	c) Assessment of seed generation procedures and verification of result-logging practices
--	---	--

The purpose of these assessments is to confirm that the RNG satisfies the applicable technical and regulatory standards required for operation on licensed platforms. Certifications are subject to periodic renewal to ensure the Operator's continued compliance.

2.5. Recognized Certification Authorities

Independent validation of the Operator's RNG systems is carried out by reputable, internationally accredited testing organisations. Bodies whose certifications are accepted include, but are not limited to:

- Gaming Associates (<https://gamingassociates.com/>)
- SIQ (<https://www.siq.si/en/>)
- Gaming Laboratory International (<https://gaminglabs.com/>)
- QUINEL (<https://www.quinel.com.mt/>)
- BMM (<https://bmm.com/>)
- Global Lab (<https://www.globaltestinglabs.com/>)
- eCogra (<https://ecogra.org/>)
- Lean Lab (<https://www.leanlab.co/>)
- itech Labs (<https://itechlabs.com/>)
- Trisigma (<https://trisigma.com/>)
- SQS (<http://soqus.com/en/>)

Certificates issued under the regulatory frameworks of the following jurisdictions are recognised, among others:

- Malta
- UK
- Spain
- Serbia
- Georgia
- Romania
- Greece

- Czechia
- Macao
- Ontario
- Poland
- Peru
- Italia
- Latvia
- Curacao
- Portugal
- Netherlands
- Isle of Man
- Lithuania
- Colombia
- Estonia

3. STORING PLAYERS' PERSONAL DATA

3.1. Data Handling and Security Infrastructure

The Operator operates a comprehensive information security framework whose purpose is to protect the personal data of players, maintain uninterrupted service availability, and fulfil the regulatory obligations arising under Curaçao's gaming supervisory framework and applicable international privacy legislation, including the GDPR. This section describes the infrastructure and procedural controls through which digital and physical assets relating to player records are protected.

3.2. Hosting Environment and Physical Safeguards

All categories of player data—comprising personally identifiable information (PII), identity verification documents, transaction records, and communications—are stored on servers housed within a Tier IV–certified data centre in Curaçao. The facility is designed with maximum fault tolerance in mind: all critical utility systems, including power, cooling, and network connectivity, are arranged in a fully redundant 2N+1 configuration that eliminates single points of failure and sustains availability approaching 100%.

The physical security of the facility is assured through layered controls: biometric authentication is required for access, continuous surveillance systems are in operation around the clock, and environmental protection is provided through precision climate regulation and automated fire suppression installations. Together, these measures safeguard against both physical interference and environmental damage.

3.3. High Availability and Regulator Access

The infrastructure is architected for continuous availability, with regulatory access requirements being a primary design consideration. Continuity of service is achieved through mirrored server configurations, dedicated backup systems, and load-balanced network links. Where a component failure occurs, automated failover processes engage immediately, ensuring that access to stored data is not interrupted.

Data is replicated in real time so that both current records and historical archives are available on demand. This architecture allows the Curaçao Gaming Authority (CGA) to retrieve records at any time, including during unplanned disruptions. Overall system availability across critical components is sustained consistently above 99.99%.

3.4. Data Security Measures

Protection of data is achieved through a comprehensive, multi-layer encryption framework covering both data in storage and data in transit:

- **At-Rest Encryption:** Stored data is encrypted using robust cryptographic standards, including AES-256. Keys are managed under strict policies governing their lifecycle and the conditions of access.
- **In-Transit Encryption:** All data exchanged between systems—whether traversing internal networks, flowing to third-party processors, or transmitted to end-user devices—is secured through transport layer protocols such as TLS/SSL, guarding against interception, unauthorised modification, and surveillance.
- **Data Integrity Assurance:** Cryptographic techniques including hashing and digital signatures are applied to confirm that stored data has not been altered without authorisation. Automated integrity monitoring operates continuously to preserve the fidelity of records.

3.5. Access Management and Activity Logging

Controlled Access: Access to systems containing personal data is assigned according to the principle of least privilege and operational need. Each user's permissions correspond to the requirements of their role: operational staff are excluded from financial data environments, while audit functions operate with read-only access. Accounts carrying elevated privileges require multi-factor authentication and are governed by rigorous password management protocols.

Audit Trails: Every action taken in relation to personal data is captured automatically in immutable audit log entries, each recording the precise timestamp, the identity of the user, and the nature of the action performed. These logs are reviewed regularly for any anomalies and are retained securely, providing full traceability for internal governance and regulatory purposes.

3.6. Backup and Recovery Strategy

The following arrangements are maintained to prevent data loss and enable prompt restoration of services:

- Complete daily backups are taken, supplemented by transaction log captures on an hourly basis.
- All backup copies are encrypted and stored in geographically separate off-site locations.
- Recovery procedures are subjected to regular testing to confirm their readiness for deployment in an emergency.

This approach is consistent with established industry standards for disaster recovery, and enables the Operator to resume normal operations with minimal disruption following any failure, security event, or loss of infrastructure.

3.7. Personal Data Governance and GDPR Alignment

The Operator's data protection practices are aligned with both the Curaçao gaming regulatory framework and the requirements of the European Union's General Data Protection Regulation (GDPR). The core elements of that approach are as follows:

Data Minimisation and Purpose Limitation: Only information that is necessary for clearly defined operational purposes is gathered and retained. The permitted purposes include account management, responsible gaming compliance, AML/KYC procedures, and the provision of contracted services. Use of data is strictly limited to those purposes.

Player Rights Management: Data subjects are entitled under the GDPR to access their personal data, to have inaccurate data corrected, and to request its erasure where appropriate. The Operator has procedures in place to ensure these requests are handled within the applicable regulatory deadlines.

Risk Assessment Protocols: In relation to processing activities carrying elevated privacy risks—such as large-scale profiling exercises or the introduction of new identity verification systems—the Data Protection Officer (DPO) is responsible for overseeing the conduct of a Data Protection Impact Assessment (DPIA) to identify risks and determine appropriate mitigations.

Compliance Documentation: Documentation of security measures, access controls, training programmes, and audit outcomes is maintained in an organised and accessible form, providing the evidential basis required for demonstrating compliance and discharging accountability under regulatory supervision.

3.8. Data Retention and Secure Disposal

Personal data is retained only for as long as is required by applicable law or by the Operator's internal policies. Pursuant to Curaçao anti-money laundering legislation, financial and transactional data is typically subject to retention periods of between five and seven years.

Once the relevant retention period has expired, or upon the confirmed closure of a player's account, the data in question is permanently deleted or rendered irreversibly anonymous by means of approved secure disposal techniques. These include cryptographic key destruction, secure overwrite routines, and physical destruction of decommissioned storage media through degaussing or mechanical shredding.

Each deletion event is recorded, and those records are retained for audit purposes. This practice gives effect to the GDPR's storage limitation principle, ensuring that no personal data is held beyond the period for which a legitimate processing purpose exists.

4. VISUAL INTERFACE ELEMENTS PRESENTED TO PLAYERS VIA PLATFORMS

Both the Operator's website and its mobile application are built on a structured visual design framework whose overriding aims are clarity, accessibility, and compliance with applicable regulatory obligations. Each component of the interface is developed with the following core purposes in mind:

4.1. Purpose of Visual Presentation

Player Engagement	Transparency and Clarity	Player Protection
The platform is designed to deliver a fluid, intuitive user journey that draws players into exploring the full range of available content and services	Terms, features, and policies are presented in a visually accessible way so that players are well informed at every point during their engagement with the platform	The design actively supports responsible gaming objectives by making applicable restrictions visible and ensuring that support resources are within immediate reach for users who may require assistance

Although certain elements of individual pages may be adapted to suit particular content or promotional contexts, a defined set of visual components is maintained consistently and without interruption across all areas of the platform, ensuring a uniform and legally compliant experience for every user.

4.2. Static UI Components

The following elements appear across all pages of the website and mobile application without exception. Their permanent presence and positioning are determined by the platform's UX/UI standards and are not contingent upon the content of any specific page.

• Header Components

The header area displayed at the top of each page includes:

Main Navigation Tabs	Direct links providing immediate access to all primary game categories available on the platform, including slot games, live casino tables, and sports wagering
Account Access	A shortcut to the user's personal account and integrated wallet, allowing the user to view their current balance and manage preferences and account settings
Brand Logo	Displayed in a consistent and prominent position to establish and reinforce the platform's brand identity
Localization Controls	Options that allow users to select their preferred interface language and to view the correct local time for their region

• Footer Components

The footer, rendered at the base of every screen, carries essential compliance disclosures and support resources, including:

Age Restriction Notice	A clearly visible reminder that platform access is restricted to individuals who have reached the minimum legal gaming age
-------------------------------	--

Licensee Details	The full registered corporate name and official address of the Operator
Licensing Information	The applicable licence number, together with a statement confirming the platform's regulation by the Curaçao Gaming Authority (CGA)
Responsible Gaming Access	A direct link to the platform's Responsible Gaming Policy and to relevant external assistance resources
Regulatory Seals	The digital compliance certification badge issued to the platform by the CGA
Terms & Conditions	Structured references to the principal legal policies of the platform, covering deposits, withdrawals, bonuses, and related matters
Social Media Links	Icons providing access to the Operator's official social media accounts, used for operational updates and customer communications

4.3. Design Consistency and Regulatory Alignment

All interface elements are deployed in accordance with the Operator's internal UX/UI standards, guaranteeing consistency of placement, visibility, and operation across all sessions and devices. Periodic aesthetic updates may occur, but the availability and accessibility of all prescribed components remains constant, fulfilling legal obligations and ensuring that users can always navigate the platform with ease.

5. ACCESS RESTRICTION CONTROLS FOR PROHIBITED INDIVIDUALS

In fulfilment of its legal obligations and its commitment to responsible gaming, the Operator has put in place a layered system of technical controls designed to prevent access by users who are disqualified from participation—whether by reason of a regulatory prohibition or through their own voluntary self-exclusion. These controls span multiple functional layers of the platform and are kept under regular review to ensure ongoing alignment with the applicable legal framework and evolving industry standards.

5.1. Age Restriction Enforcement

Mandatory Date of Birth Declaration	At the point of account creation, users are required to supply their complete date of birth. The platform processes this information automatically to verify that the applicant satisfies the minimum age of 18 years required by law
Automated Identity Verification	The platform may, as part of its age confirmation and anti-fraud procedures, require the submission of government-issued photographic identification. Documents are examined using certified

	third-party KYC solutions to verify their authenticity and confirm that the age requirement is met
Manual Review by Compliance Personnel	In cases where automated verification does not yield a definitive result, the Compliance Team undertakes a manual review of the submitted documentation to reach a determination on the applicant's eligibility
Immediate Suspension of Underage Accounts	Where it is confirmed at any stage that an account is held by a person below the minimum legal age, the account is closed with immediate effect and all associated activity and financial transactions are voided in accordance with the applicable Terms and Conditions

5.2. Geographic Access Restrictions

IP-Based Location Monitoring	The platform uses automated geolocation technology to determine the jurisdiction from which each user is connecting. Access is blocked immediately for any user attempting to connect from a territory in which online gambling is prohibited or in which the Operator lacks the requisite authorisation to operate
Dynamic Territory Restrictions	The register of prohibited jurisdictions is continuously maintained and updated. Where changes in applicable law or licensing conditions require new restrictions, these are implemented promptly across the platform
Enforcement of Regional Bans	Any user identified as connecting from a prohibited territory is denied access. Accounts confirmed to be in breach of geographic access controls may be suspended, with associated transactions voided, in accordance with the Operator's policies

5.3. Identity and Account Integrity

Verification of Contact Details	New users are required to verify their email address or mobile telephone number by responding to a verification link or entering a one-time passcode (OTP) sent to the relevant contact, confirming both the accuracy of the details and the registrant's ownership of them
Detection of Duplicate Accounts	The Operator enforces a one-account-per-user policy, with automated systems screening new registrations against shared indicators such as IP address patterns, device fingerprint data, and similarities in personal information. Potential duplicates are flagged for review by the compliance function

Manual Review of Identification	Where automated identity verification procedures are unable to reach a definitive outcome, the Compliance Team reviews submitted documentation manually to confirm the user's identity and eligibility
Know Your Customer (KYC) Triggers	Full identity verification is initiated in any of the following circumstances: • On the user reaching a specified cumulative deposit threshold • Prior to the processing of the user's first withdrawal • On identification of suspicious or irregular account behaviour • As part of a scheduled periodic review of the account

5.4. Device Identification and Session Management

Device Profiling	The platform records technical characteristics of each user device on connection—including browser type, screen specifications, operating system, and installed browser extensions—to create a session-level fingerprint. This data is used to detect attempts to create or operate multiple accounts from the same device and to trigger appropriate enforcement measures
Login Session Oversight	Concurrent logins from multiple devices are generally not permitted. Where access is sought from an unrecognised device or from a new geographical location, the user may be required to complete additional verification before access is granted
Inactivity-Based Logout	Active sessions are automatically closed after a period of inactivity, reducing the risk of unauthorised access where a device is shared or left unattended

5.5. Login Protection Measures

Multi-Factor Authentication (MFA)	The platform offers users the option to enable MFA, which supplements standard password credentials with a verification code delivered via an authenticator application or SMS
Login Attempt Surveillance	The system monitors failed login attempts and, once a defined threshold is exceeded, temporarily suspends the relevant account and refers it for investigation by the security team
Automated Threat Prevention	CAPTCHA technology is integrated into both the login and registration workflows, preventing bot-driven automated access and protecting the platform against scripted abuse

5.6. Fraud Monitoring and Behavioral Analysis

User Behavior Monitoring	Ongoing analytical systems assess player behaviour across all observable dimensions—deposits, wagering, withdrawals, and session patterns—to identify deviations that may indicate fraudulent activity or misuse of the platform
Real-Time Risk Alerts	Certain categories of activity—including unusual shifts in access location, use of payment methods linked to prior concerns, or unusually rapid transaction sequences—generate immediate automated alerts for review by the Operator’s fraud management team
Transaction Rate Controls	Velocity limits are applied to financial transactions on the platform in order to deter automated activity and to flag sudden changes in a user’s behavioural profile that may be consistent with account compromise or systematic exploitation

5.7. Enforcement Against Prohibited Users

Voluntary Exclusion Controls	Users who have applied for self-exclusion or who are within a designated cooling-off period are prevented from accessing their accounts and from conducting any form of wagering or financial activity on the platform
Internal Blacklisting	Accounts associated with confirmed breaches of the Operator’s policies—including chargeback abuse or identity fraud—are placed on a secure internal restricted list and permanently denied access to the platform

6. TECHNICAL INFRASTRUCTURE OVERVIEW AND EMERGENCY RESTORATION CAPABILITIES

The Operator’s technology environment is designed with operational resilience as its central objective. Fault-tolerant infrastructure, structured recovery procedures, and robust backup arrangements work together to ensure that services can be maintained even in the event of technical failure, security incidents, or disruption to physical facilities.

6.1. Core Systems and Hosting Setup

The services most critical to the Operator’s operations—encompassing financial processing, administrative systems, and the gaming platform—are hosted within an internally managed data centre, which is equipped with:

a) Secure, access-controlled server rooms	b) A virtualised server infrastructure allowing for flexible and scalable resource management	c) Systematic backup procedures to ensure data recoverability and the continuity of all critical operational functions
---	---	--

6.2. Network Structure and Backup Strategy

The network is designed to deliver continued connectivity and to support rapid service restoration in the event of disruption:

a) Dedicated routing and switching hardware maintained in readiness	b) Regularly scheduled backups of critical data sets and all system configuration files	c) Stored configuration archives that can be used to reconstruct network settings promptly following any failure or security compromise
---	---	---

6.3. Disaster Recovery Procedures

Upon identification of a system failure or physical incident, the Operator implements a phased and structured recovery programme. Responsibility for each phase is allocated in advance to designated personnel, and procedural checklists are available to support efficient execution:

Hardware Recovery	Malfunctioning components are identified and replaced from on-site spare parts or pre-staged standby units; contact details for equipment suppliers are maintained for emergency procurement where necessary
System Recovery	Production systems are reinstated from verified, clean backup images; application data is restored and all available security patches are applied
Network Restoration	Connectivity is re-established by switching to backup ISPs and reconfiguring VPN configurations; network monitoring and alerting systems are brought back online
Communication Tools	In the event of email system unavailability, communications are redirected to cloud-hosted alternatives; telephone systems are forwarded to mobile devices and voicemail recordings are updated to reflect current operational status
Endpoint Access	Once central systems are restored, staff workstations are rebuilt using standard imaging procedures and secure remote access credentials are distributed to authorised personnel

6.4. Staff Coordination and Communication

The following arrangements are maintained to ensure effective coordination and rapid decision-making throughout an incident:

a) A designated Incident Lead takes	b) Functional team leaders oversee	c) Communication is maintained through	d) Progress updates and operational resources
-------------------------------------	------------------------------------	--	---

overall command, activates the recovery programme, and coordinates all aspects of the organisational response	recovery activity in their respective domains: IT (systems and data), Administration (logistics), Facilities (physical environment), and Communications (internal and external messaging)	multiple parallel channels—telephone, SMS, email, and messaging applications—to ensure that all staff can be reached even where primary systems are disrupted	are communicated through pre-scheduled briefings or live status dashboards; pre-drafted message templates for incident notifications and public communications are prepared in advance and ready for immediate deployment
---	---	---	---

Figure: Technical Infrastructure and Emergency Recovery Model

7. RESPONSIBLE GAMING

The Operator is steadfastly committed to maintaining a gaming environment that protects players from harm and upholds rigorous ethical standards throughout all aspects of its operations. Its responsible gaming policies are designed to satisfy the regulatory requirements of Curaçao and to reflect leading practice in the protection of vulnerable individuals, the exclusion of minors, and the promotion of well-informed, autonomous decision-making by players.

7.1. Objectives of Responsible Gaming

The Operator's Responsible Gaming programme is established in pursuit of the following objectives:

- To position gaming as a form of entertainment, clearly distinguishing it from a means of earning income.
- To prevent the platform from being accessed by persons below the legal age or by any other category of excluded individual.
- To detect early signs of problematic gambling and to respond with proportionate and effective interventions.
- To give players practical tools through which they can exercise meaningful self-regulation and, where necessary, self-exclusion.
- To ensure that both players and staff possess adequate knowledge of the risks associated with gambling and of the protective resources available.
- To fulfil all applicable regulatory requirements and the conditions attached to the Gaming Licence without exception.

7.2. Player Information & Transparency

Responsible Gaming (RG) information and resources are made prominently and easily accessible throughout all user interfaces. The RG Policy is available in multiple languages and is woven into the registration journey, account management settings, and help documentation.

Players can access the following at any time:

- Clear explanations of the tools available to support responsible play, including deposit limits, session time-outs, and self-exclusion options.

- Guidance on responsible gambling behaviour, including guidance on identifying warning signs of problematic play and information about external support organisations.
- Tools that allow users to track session duration and to review their transaction history on a real-time basis.

7.3. Age Verification Controls

The Operator applies the following measures to prevent minors from accessing the platform:

Confirmation of age is a mandatory requirement at the registration stage.

Date of birth, supporting identity documentation, and proof of ownership of the nominated payment method are all subject to verification.

Government-issued photographic identification (such as a passport or driving licence) is required before any withdrawal is processed and upon the occurrence of defined trigger events, including reaching a cumulative deposit threshold.

Accounts confirmed as belonging to minors are closed with immediate effect, refundable funds are returned, and all associated activity is reversed.

The Operator recommends the use of parental control software (for example Net Nanny or CyberSitter) on devices shared between adults and children, as an additional safeguard.

7.4. Tools for Player Self-Control

A comprehensive set of configurable tools is available to help users manage and moderate their gambling activity:

- **Deposit Limits:** Maximum deposit thresholds may be set on a daily, weekly, or monthly basis. Reductions apply immediately; increases are subject to a mandatory seven-day waiting period before taking effect.
- **Loss & Wager Limits:** Where the platform supports it, users may apply limits to total losses or wagering volume over a specified period.
- **Session Timers:** An active session clock is displayed to users in the course of gameplay.
- **Reality Checks:** Automated notifications are sent at regular intervals, summarising the time that has elapsed and the user's net result for the session.
- **Cooling-Off Periods:** Users may choose to suspend their account for a period of 24 hours, 7 days, one month, or three months, during which login access and wagering are disabled and marketing communications are suspended.

7.5. Self-Exclusion Program

Self-exclusion is offered across all of the Operator's products and platforms and takes effect from the moment of application. Users may select a fixed exclusion term of 1, 3, 5, or 10 years, or may opt for permanent exclusion.

The following conditions govern the self-exclusion programme:

- Self-exclusion can be initiated by the user directly through their account, without any requirement to engage with staff.
- Excluded accounts are locked out of all services provided by the platform, including deposits, wagering, and account management functions.

- Payment instruments associated with the account are placed on a restricted list to prevent the exclusion from being circumvented.
- Exclusion records are entered in the Self-Exclusion Register and retained for a minimum of seven years following the conclusion of the exclusion period.
- An exclusion cannot be revoked or curtailed before its stated expiry.
- Reactivation at the end of the exclusion period requires the user to submit a written request, to receive responsible gaming guidance, and to complete a gambling behaviour questionnaire.

Self-exclusion may be applied to:

- Selected product verticals only (for example, casino games or sports betting).
- The full platform and every domain operated in connection with it.

7.6. Monitoring and Detection of Risk

Player behaviour is monitored on a continuous basis through a combination of automated risk detection tools—incorporating AI and machine learning capabilities—and manual oversight by trained staff.

Behavioural indicators reviewed include:

- Unusually elevated deposit or wagering frequency.
- Withdrawal requests that are subsequently cancelled or reversed.
- Reliance on several different payment instruments within a short period.
- Repeated changes to responsible gaming settings or limits.
- Extended play sessions conducted without any break.
- Evidence of attempts to open or operate more than one account.
- Behavioural patterns that give rise to concern in relation to younger users.

Accounts that trigger risk indicators are referred to the Responsible Gaming team for further assessment and, where warranted, escalated for direct intervention.

7.7. Intervention Procedures

Where there is a reasonable basis to suspect harm or misuse, the Operator takes the following steps:

- Trained responsible gaming staff contact the player and offer appropriate support, which may include the setting of limits, activation of a time-out, or engagement of the self-exclusion mechanism.
- Players may be directed to external assistance services, including national helplines and accredited counselling organisations.
- In appropriate cases, the Operator may unilaterally restrict account access to prevent further harm to the player.
- All interventions are recorded in the Player Account Management system, enabling ongoing monitoring and providing a compliance record for regulatory purposes.
- Where a serious and immediate risk is identified, the Operator may impose mandatory exclusion or permanently close the account.

7.8. Staff Training and Role Definition

All frontline personnel—in particular customer service staff and VIP account managers—receive annual training that addresses:

- How to identify behavioural signs of distress or problem gambling in players.
- How to approach and conduct sensitive player conversations with empathy and professionalism.
- How to communicate and provide access to the support tools and resources available on the platform.
- How to document interactions accurately and to refer concerns through internal escalation processes.

The training curriculum is reviewed every year and revised as required, taking into account findings from internal audits, player feedback, and the evolution of regulatory requirements and industry best practice.

7.9. Marketing and Communication Restrictions

The Operator's marketing activities are conducted subject to the following responsible gaming constraints:

- Marketing communications are not directed to players who are self-excluded or who are within a cooling-off period.
- All marketing to any affected user ceases immediately upon the activation of self-exclusion or a cooling-off measure.
- Promotional content is not targeted at minors or at users identified as vulnerable or high-risk.
- Gambling is not portrayed in any marketing material as a means of generating income or as a reliable financial opportunity.
- All affiliate and influencer partners are bound contractually to comply with applicable age restrictions, content standards, and restrictions on audience targeting.

7.10. Compliance and Regulatory Reporting

The Operator maintains full records of all responsible gaming interactions, exclusion events, and reportable incidents. In the event that a self-excluded or underage user gains access to the platform, the following procedure is applied:

- The account is blocked as soon as the breach is identified.
- Any deposits not subject to AML restrictions are refunded to the user.
- An incident report is submitted to the Curaçao Gaming Authority (CGA) within twenty-four (24) hours of discovery, pursuant to Article 5.10, sixth paragraph, of the National Ordinance on Games of Chance.
- The Operator may additionally impose exclusion measures where there is reliable evidence of abusive conduct, criminal activity, or a pattern of excessive gambling.

8. TERMS AND CONDITIONS

This section sets out in full the current text of the general terms and conditions (the "Terms and Conditions") applicable to players, as required by Article 5.9, first paragraph, letter h, of the National Ordinance on Games of Chance. The Terms and Conditions constitute the contractual basis of the

relationship between the Operator as licence holder and each individual player, and their acceptance is required at the point of registration and following each material amendment.

8.1. Mandatory Content

In conformity with the National Ordinance on Games of Chance and the conditions attached to the Gaming Licence, the Terms and Conditions address, as a minimum requirement, the following subject matters:

- Governing law and jurisdiction: the gaming agreement is subject to Curaçao law, and all disputes arising under or in connection with it shall fall within the jurisdiction of the courts of Curaçao (Article 5.5).
- Eligibility and prohibited persons: a mandatory minimum age of eighteen (18) years for all players, and the exclusion from participation of Vulnerable Persons and any other persons disqualified under the National Ordinance (Articles 1.4 and 5.4).
- No credit: the Operator provides no credit to players and acts as no intermediary in securing or arranging credit on a player's behalf (Article 1.4, letter c).
- Account registration, identity verification (KYC), and the player's continuing obligation to provide true and complete information.
- Deposits, withdrawals, accepted payment methods, applicable currency, and the requirement that only payment instruments in the account holder's own name may be used for transactions.
- Minimum and maximum wagering limits per player and per bet, all other conditions of participation, and the means by which prizes are determined and player credits are paid out (Article 5.8, letters f, g, and h).
- The games available on the platform, the rules and paytables applicable to each, and the handling of technical malfunctions, invalidated bets, and connection failures.
- Bonuses, promotional offers, and associated wagering requirements, structured to avoid encouraging excessive play, to avoid misleading players, and not to target Vulnerable Persons (Article 5.6).
- Responsible gaming controls and self-exclusion rights, including the player's right to request exclusion in writing for a period of not less than twelve (12) months (Article 5.4).
- Complaints handling and alternative dispute resolution, with cross-reference to Section 9 (Dispute Resolution) of this Manual and to Article 5.3.
- The use and protection of personal data, with cross-reference to Section 3 (Storing of Players' Personal Data) of this Manual.
- The treatment of inactive accounts, account closure, and the consequences of any breach, including the invalidation of transactions and closure of accounts held by minors or prohibited persons.
- The procedure for amending the Terms and Conditions, the means by which players are notified of any changes, and the effective date of the version currently in force.

8.2. Current Text of the Terms and Conditions

<http://clickpari.com> (the "Website") is operated by LOTOSTORM B.V., a company incorporated under the laws of Curaçao with Company Number 163910, registered at 03, Abraham Mendez Chumaceiro Boulevard, Willemstad, 4750, Curacao, and licensed by the Curaçao Gaming Control

Board to offer games of chance under license number OGL/2024/303/0300 (the “Company”, “We”, “our”, “us”) in accordance with the National Ordinance on Offshore Games of Hazard (Landsverordening op de kansspelen, P.B. 2024, no. 157) since 02/09/2025.

Payments are processed by WOOLFEATWOLF LIMITED, registration number HE 448601 registered at 11, Filippou, Agios Dometios, Nicosia, 2363, Cyprus acts as payment agents on behalf of LOTOSTORM B.V.

For the purposes of these Terms of Service, the user and, wherever the context requires “you”, “your” means the person who accesses the Website, its content and uses the gaming and other services (the “Services”) offered on or through the Website (the “Customer”, “you”, “your”).

The following Terms of Service pertaining to us stipulate the manner of accepting bets, paying winnings and resolving disputes, as well as the specific features of certain bets on certain sports. These Terms of Service shall govern any other relations between the Company and the Customer. These Terms of Service shall apply to betting on the Website and at the Company betting facilities.

“Bet” is a risk-driven agreement for potential winnings entered into between the customer and the bookmaker under the established Rules, where the fulfillment of such agreement is conditioned by an event whose outcome is yet to be determined. Bets are accepted on the conditions offered by the bookmaker.

“Bonus” is a promotional reward offered by the Company to Customers. Bonuses may include extra funds, free spins, or other incentives and are subject to specific terms such as deposit requirements, wagering conditions, and expiration periods accordance with these Terms of Service.

“Privacy Policy” is policy on the collection, processing, use, and protection of personal data, as described in Section 29 (Privacy & Management of Personal Data).

“Security Service” or “Security Team” is the internal division of the Company responsible for monitoring and ensuring the integrity of financial transactions, including deposits and withdrawals.

“Support Service” is the Company’s official customer assistance channel, available for handling inquiries, complaints, account-related issues, refund requests, and other communications from the Customer. All communication with the Support Service shall be directed via email to support-en@clickpari.com.

“AML” (Anti-Money Laundering) is a framework of laws, regulations, and procedures established to detect and prevent money laundering and related financial crimes.

“CTF” (Counter-Terrorism Financing) is the process of identifying, preventing, and disrupting financial transactions intended to support terrorist activities.

“KYC” (Know Your Customer) is procedures used to verify the Customer’s identity and monitor their financial behavior as part of regulatory compliance.

“Outcome” is the result of the event (events) on which the bet was placed.

“Bet Cancellation” is an outcome on which the bet is not settled and winnings are not paid. As per the Terms of Service, in the event of “bet cancellation”, an arrangement between the Company and the customer shall be deemed unconcluded and the stake shall be refunded.

“Regular Time” is the duration of the match subject to the regulations of the relevant sport, including time added by the referee. Regular time does not include extra time, overtime(s), penalty shootouts, etc.

In order to register for this Website, the Customer is required to accept the Terms of Service. In the event the Terms of Service are updated, existing users may choose to discontinue using the products and services before the said update shall become effective, which is a minimum of two weeks after it has been announced. In addition to the English language, copies may also be available in other languages. In the event of discrepancies between the English version and any translated version of these Rules, the English version shall prevail. Translations are provided for convenience only.

By registering, you confirm that you are acting on your behalf and not on behalf of any third party. You declare that you are the ultimate beneficial owner of the account and funds used, and not acting as a proxy.

The following individuals are not allowed to place bets:

individuals who are under 18 years of age at the time of placing a bet, or such other minimum legal age as may be required by the applicable laws of the Customer’s jurisdiction. In all cases, the minimum age shall not be lower than 18 years;

individuals who directly participate in the events being betted on (e.g. sportspeople, coaches, referees, club owners or club management, or other individuals who can influence the outcome of the event), as well as any individuals acting on their behalf or affiliating with them;

individuals representing other bookmakers;

individuals who have problems with gambling addiction;

individuals who are prohibited from entering into a contract with a bookmaker subject to the effective legislation.

The right to access and/or use the Website (including any or all of the products offered through the Website) may be considered illegal in certain countries (including, for example, the USA, the United Kingdom, Cyprus, the Netherlands, etc.). We do not intend for our Website to be used for sports betting, gambling or other purposes by people who reside in countries or jurisdictions in which such types of activity are illegal.

The list of explicitly forbidden territories is: Australia, Curacao, France, Netherlands, Spain, the U.S.A or the U.S.A dependencies, the United Kingdom, Aruba, Bonaire, Saba.

The fact that our Website is available in such a country and/or jurisdiction or that it can be displayed in the official language of any of those countries cannot be considered official authorization or legal

grounds for using our Website and depositing funds into your account or withdrawing your winnings. The availability of the Website does not mean that it contains any proposals, incitement or invitation to use or subscribe to betting, gambling or any of the other services in any jurisdiction where such activity is illegal.

You are responsible for determining whether your accessing and/or use of the Website is compliant with applicable laws in your jurisdiction and you warrant to us that gambling is legal in the territory where you reside. When opening an account and/or using our Website you must make sure that your actions are legal in the territory in which you reside. You confirm that you understand and accept your responsibility to comply with applicable local laws and regulations and warrant that you have sought legal advice if necessary. If we become aware that you are a resident in a country where the use of our Website is considered illegal, we will have the right to close your account and refund any remaining balance on your account at the moment of its closure (after the deduction of any winnings credited after your most recent deposit was made).

The Company shall be entitled to refuse bets from customers who fail to abide by these Terms of Service. The Company reserves the right to refuse to accept a bet of any type from any customer should they violate social standards of conduct and public order.

The Company reserves the right to refuse to accept a bet from any individual without giving a reason. All bets shall be settled based on the data provided by the processing center.

Winnings shall be paid to the bettor within 30 (thirty) calendar days from the date of official publication of the results of the latest event on the bet slip.

A bet placed by the Customer shall be deemed won if all outcomes specified in such bet have been predicted correctly.

Betting terms (odds, handicaps, totals, maximum stake limits, etc.) may be subject to variation after a bet has been made, but this does not affect the terms at the time the bet was placed. Before entering into an arrangement, the Customer shall check all changes in the current pre-match markets.

In the case of technical failures and unfinished streams, etc. bets on Esports Live will be refunded only if the event in question does not occur or bets on the event are not settled by the bookmaker.

If an employee makes an error while accepting a bet (obvious misprints on the list of events, inconsistency of odds between offered betting markets and the bet, etc), or a bet is accepted in violation of these Rules, or if there are any other indications that the bet is wrong, the Company reserves the right to declare such bets void. Returns on such bets shall be paid at odds of 1.

In the event of obviously erroneous odds, such bet shall be settled based on the final result at the effective odds applicable to the certain market.

In the event of suspicions in the unsportsmanlike format of matches the company reserves the right to block bets on sport event before final conclusion of an international organization and declare bets as invalid if the fact of an unsportsmanlike game is determined. Payment of these bets is made with odds "1". The administration is not obliged to present evidence and conclusions to the customers.

The Company is committed to ensuring fair play in sport and is fully aware that the manipulation of sporting events (as well as other events) is linked to committing criminal acts (organized match fixing, corruption etc.) including organized criminal activities, as well as transnational and cross-border organized crime. Consequently, the Company fully complies with the goals and main objectives of the “Council of Europe Convention on the Manipulation of Sports Competitions” (CETS No.215), as well as relevant legislative requirements.

The Company is entitled to void bets if there is any suspicion or confirmation of foul play (match fixing), bets being placed using another Customer’s account, the use of a Customer’s account by a third party or any unusual betting activity (i.e. any differences in the type, size, volume and manner of bets placed).

The term “foul play” refers to the favorite intentionally losing a match or match fixing as defined by the rules of a competition for financial, competitive or other reasons, as well as any other violation of the rules of the relevant sport.

Should these Terms of Service be amended, customers shall be notified accordingly. Bets accepted after the specified date shall be subject to the amended Terms of Conditions. Earlier bets shall remain unchanged.

No connection failure while receiving confirmation of a bet shall entail the cancellation of such bet.

Placing a bet acts as proof that the Customer agrees to and accepts these Betting Rules.

Bets shall be settled and winnings shall be determined based only on the results declared by the Company. Any complaints about the results, date, and actual starting time of the event shall be considered together with official documents from the relevant sports federations.

No complaint in connection with or arising from transliteration (or translation) of a team name, player’s surname, or sports venue will be considered by the Company. A tournament title is given for convenience only. No mistake in a tournament title shall result in a stake refund.

In no event shall the Company be held liable to the Customer for any indirect, collateral, or incidental losses or damages (including loss of profit), even though they may have been notified that such losses or damages are likely to occur.

The Company reserves the right to update these Terms of Service and add new provisions at any time. Such new terms or amendments shall take effect immediately after publication on the Website.

The Company customers are informed about the odds of winning and of the potential consequences and risks of losing.

Your withdrawals and deposits can be accessed through the “My Account” section.

9. DISPUTE RESOLUTION

The Operator processes all player complaints and disputes in accordance with Article 5.3 of the National Ordinance on Games of Chance. Complaints are accepted without charge and are handled in a manner that is equitable, transparent, and consistent with the statutory response deadlines set out below.

9.1. Filing a Complaint

- A player may bring a complaint to the Operator without incurring any charge, provided it is submitted within six (6) months of the date on which the incident giving rise to the complaint occurred in connection with the player's participation in a Game of Chance.
- Complaints must be submitted using the Operator's approved complaint form, which is consistent with CGA guidelines and requires the following information: the complainant's full name, postal address, and place of residence; the date of the complaint; submission in one of the designated official languages (English, Dutch, or Papiamentu); and a clear description of the conduct that forms the basis of the complaint.

9.2. Acknowledgment and Handling

- Within one (1) week of receiving a complaint, the Operator will send the complainant written confirmation of receipt along with a description of the procedure that will be followed in addressing it.
- Within four (4) weeks of receipt, the Operator will notify the complainant of either: (a) a decision not to proceed with the complaint, accompanied by reasons; or (b) the substantive outcome of the complaint, with supporting details, in written form.
- This four-week period may be extended once by written notification to the complainant, for a further period of four (4) weeks.

9.3. Alternative Dispute Resolution (ADR)

- The Operator makes alternative dispute resolution available to players at any point in the process, without charge to the player. ADR services are provided by a body accredited by the CGA, and all associated costs are borne by the Operator.
- Without prejudice to the availability of ADR, all disputes arising under the gaming agreement are subject to Curaçao law and may be referred to the courts of Curaçao for determination (Article 5.5).

9.4. Records

- The Operator records every complaint received, the steps taken in response, and the outcomes reached, and preserves those records in a form that permits production to the CGA upon request. Complaint statistics are incorporated into the periodic regulatory reports submitted to the CGA (Article 5.10).

The CGA-approved alternative dispute resolution (ADR) body engaged by the Operator is:

CADRE (Curaçao Alternative Dispute Resolution Entity) – independent iGaming dispute-resolution provider.

Website: cadre.online

Contact: operators@cadre.online

A player who remains dissatisfied following the conclusion of the Operator's internal complaints procedure may refer the dispute to CADRE, at no cost to the player.

10. STORAGE OF DIGITAL RECORDS FOR CRITICAL OPERATIONAL DATA

The Operator maintains comprehensive, durable digital records of player activity, financial transactions, and account information, in compliance with all applicable regulatory obligations and on a long-term basis.

10.1. Data Format and Content

Transaction records are exported from the Operator's platform at regular intervals and stored in structured digital file formats (.csv or .xlsx), in conformity with the requirements of the Curaçao Gaming Authority (CGA).

Each stored record must contain the following mandatory fields: player Account ID; player Account Country; transaction ID; date of transaction; currency; transaction amount; and payment method. All such files are retained for a minimum period of five (5) years.

10.2. Storage Infrastructure and Access

All digital records are held on encrypted servers located within a Tier IV–certified data centre in Curaçao. Access is controlled by appropriate authentication mechanisms, such as username and password credentials or equivalent access management systems.

The CGA must be able to access these servers at all times, whether through the provision of administrative credentials or by means of a pre-authorised secure access arrangement.

Pursuant to Article 4(1) of Regulation (EU) 2016/679 (the General Data Protection Regulation), the stored transaction records are personal data and must be treated as such by the Operator's own staff and by any contracted data hosting provider. This obligation encompasses ensuring the confidentiality, integrity, and security of the data throughout its entire lifecycle.

11. PERMANENT EDUCATION, MANUAL MAINTENANCE, AND REGULATORY REPORTING

This section sets out the Operator's procedures for maintaining this Operational Manual in a current and accurate state, for delivering training to staff, and for meeting its reporting obligations to the Curaçao Gaming Authority (CGA) under Articles 5.9, 5.10, and 5.11 of the National Ordinance on Games of Chance.

11.1. Permanent Staff Education (Article 5.9, fourth paragraph)

The Operator delivers annual training to all members of staff whose roles relate to the operation of Games of Chance. The training is tailored to each person's role and reflects the standard of knowledge

and competence that is expected of someone in that position. The curriculum addresses, among other subjects:

- mental well-being;
- anti-bribery compliance;
- crime prevention;
- responsible gaming;
- anti-money laundering (AML) and countering the financing of terrorism;
- effective communication with players; and
- the responsible conduct of advertising activities.

Participation and completion records are maintained by the Operator and are made available to the CGA upon request.

11.2. Maintenance and Inspection of the Operational Manual (Article 5.9, paragraphs 2 and 3)

- The Operator is responsible for ensuring that this Operational Manual is kept accurate and up to date at all times. Where the CGA has published approved templates for operational manuals, the Operator uses those templates in preparing and revising this document.
- Upon receiving an initial request from the CGA, the Operator makes the Operational Manual available for inspection within five (5) working days.

11.3. Reporting to the CGA (Article 5.10)

- Amendment reports: the Operator notifies the CGA of all revisions made to this Operational Manual and provides a copy of the updated document. Such reports are submitted on a biannual basis, no later than 15 June and 15 January of each year.
- Incident reports: within twenty-four (24) hours of its occurrence, the Operator reports to the CGA any security breach, equipment or software failure, gaming-related fraud or other criminal conduct, and any other event that materially undermines the responsible, reliable, or verifiable conduct of Games of Chance. Each report describes the measures taken in response.
- Gambler transaction reports and complaint reports: the Operator submits reports on player transactions and complaints, and provides any further information that the CGA determines to be necessary for supervisory purposes, using the formats and submission channels designated by the CGA.

11.4. Record-Keeping and Financial Statements (Article 5.11)

- The Operator maintains records of its Games of Chance activities in a manner that clearly reflects, at all times, the rights and obligations of the Operator and the entitlements of each player, and that allows the Operator to respond to any CGA data request within a reasonable period.
- Annual financial statements are submitted to the CGA by 30 June of the year following the close of the relevant reporting period. Interim reports are provided as and when the CGA considers this to be necessary.

The individual accountable for this Operational Manual and for all obligations arising under Articles 5.9, 5.10, and 5.11 is the **Compliance Officer, Semen Klyuchyik** (email: semenklyuchyik@gmail.com). The Compliance Officer's responsibilities encompass:

- managing and delivering the annual staff training programme for all personnel engaged in the Games of Chance field, and maintaining records of attendance and completion (Article 5.9, fourth paragraph);
- exercising version control over this Operational Manual to ensure it remains accurate and current, with each amendment documented by version number and effective date (Article 5.9, paragraphs 2 and 3); and
- fulfilling each reporting obligation owed to the CGA—comprising amendment reports, incident reports, gambler-transaction and complaint reports, and annual financial statements—and responding to any additional information requests made by the CGA (Articles 5.10 and 5.11).