

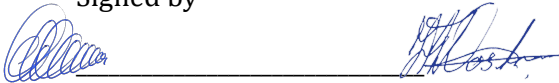
Operational Manual

Castianes B.V. (the “Company”)

VERSION CONTROL

Version	Version Effective Date	Approved By (Approving Officials)
1.0	16.06.2026	The Board

Signed by

Two handwritten signatures in blue ink, one on the left and one on the right, positioned above a horizontal line.

on behalf of e-Management N.V., Director

CONTENTS

VERSION CONTROL.....	2
CONTENTS	3
1. DEFINITIONS AND ABBREVIATIONS	6
2. SCOPE	9
2.1 Introduction.....	9
2.2 Purpose.....	9
2.3 Amendment Process.....	9
3. GAMES OF CHANCE.....	10
3.1 Description of Games of Chance	10
3.2 Payment Methods.....	11
3.3 Bet Settings and Parameters.....	12
4. SYSTEM TESTING AND ACCEPTANCE	13
4.1 Protection of System Test Data.....	13
5. THE WAY OF STORING PLAYERS' PERSONAL DATA AND OTHER DETAILS	15
5.1. Regulatory Requirements	15
5.2. Data Storage Infrastructure.....	15
5.3. Categories of Personal Data and Retention Periods.....	15
5.4. Security Standards	17
5.5. Data Protection Compliance.....	17
6. VISUAL REPRESENTATION OF PLAYER INTERFACE ELEMENTS	18
7. TECHNICAL INFRASTRUCTURE AND DISASTER RECOVERY PLAN	32
7.1 Non-Functional Requirements (NFRs) for Every Service.....	32
7.1.1 Backup and Recovery Plan Requirements.....	32
7.1.2 High Availability (HA) Requirements	33
7.1.3 Data Criticality Definitions	33
7.1.4 Briefly described requirements depending on the data criticality.....	35
7.1.5 Separated Locations Requirement.....	36
7.2 Periodical Data Restoration Testing	36
7.2.1 Scope of Testing.....	37
7.2.2 When to Perform	37
7.2.3 Definition of Done	38

7.2.4 Documentation and Reporting	38
7.3 Monitoring and Responding.....	38
7.3.1 Department and Team Level Monitoring.....	38
7.3.2 Questionnaire and Dashboard	39
7.4 Review and Compliance	40
7.5 Diagram of the technical infrastructure.....	40
8. PRINCIPLES OF RESPONSIBLE OPERATION	41
8.1 Prevention of vulnerable person participation.....	41
8.2. Marketing and advertising standards	42
9. TERMS & CONDITIONS	43
9.1 Scope of the Terms and Conditions.....	43
9.2 Player Acknowledgment and Amendment Procedures	44
9.3 Accessibility and Availability.....	44
9.4 Regulatory Submissions and Record-Keeping.....	44
9.5 Review and Updates	44
10. DISPUTE RESOLUTION FRAMEWORK	45
10.1 Principles.....	45
10.2 Submission and Eligibility.....	45
10.3 Handling Procedure	45
10.4 Escalation to Alternative Dispute Resolution.....	46
10.5 Policy Availability	46
11. SERVER OF A TIER-IV	47
11.1 Current Infrastructure Alignment.....	47
11.2 Operational Readiness	47
11.3 Preparatory Measures.....	47
12. STAFF TRAINING AND CONTINUOUS EDUCATION	49
12.1 Training Topics	49
12.2 Role-Based Training.....	49
12.3 Training Frequency.....	49
12.4 New Employee Onboarding.....	50
12.5 Monitoring and Record-Keeping	50
12.6 Review and Continuous Improvement.....	50
13. PLAYER ACCESS RESTRICTION MEASURES.....	51

13.1 Registration-Stage Controls.....	51
13.2 Ongoing Monitoring and Screening.....	52
13.3 Responsible Gaming Restrictions.....	52
13.4 Key Person Play Restriction.....	53
13.5 Governance and Review	53

1. DEFINITIONS AND ABBREVIATIONS

ADR (Alternative Dispute Resolution) – An independent and impartial process for resolving player complaints outside of the Company's internal complaint handling procedure, as required by the National Ordinance on Games of Chance.

AML (Anti-Money Laundering) – A framework of laws, regulations, and procedures designed to prevent criminals from disguising illegally obtained funds as legitimate income.

AWS (Amazon Web Services) – The Company's principal cloud-based data storage and processing infrastructure provider.

CGA (Curaçao Gaming Authority) – The regulatory authority responsible for the supervision and enforcement of gaming legislation in Curaçao, operating under the National Ordinance on Games of Chance.

CFT (Countering the Financing of Terrorism) – Measures and procedures implemented to prevent the use of financial systems to support terrorist activities.

DDoS (Distributed Denial of Service) – A cyberattack in which multiple compromised systems are used to target a single system, causing service disruption.

Disaster Recovery (DR) – Procedures and protocols for restoring services, systems, and data after a critical failure or emergency situation.

FATF (Financial Action Task Force) – An inter-governmental body that sets international standards for combating money laundering and terrorist financing.

FIU (Financial Intelligence Unit) – The national agency responsible for receiving, analyzing, and disseminating financial intelligence related to suspected money laundering or terrorist financing activities in Curaçao.

GDPR (General Data Protection Regulation) – Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

HA (High Availability) – System design and architecture ensuring minimal service disruption through redundancy, failover mechanisms, and continuous operation.

HoE (Head of Engineering) – The senior technical leadership role responsible for approving non-functional requirements, backup plans, and technical infrastructure decisions.

IVR (Interactive Voice Response) – An automated telephony system that interacts with callers, gathers information, and routes calls to the appropriate recipient.

Key Person – A person as defined in Article 1.1(n) of the National Ordinance on Games of Chance, including directors, supervisory directors, and other individuals in positions of significant influence or control over the licensed operation.

KYC (Know Your Customer) – Identity verification and due diligence procedures used to verify the identity of players, assess their risk profile, and comply with regulatory obligations.

LOK (Landsverordening op de Kansspelen) – The National Ordinance on Games of Chance, the principal legislative instrument governing the offering and operation of games of chance in Curaçao.

MFA (Multi-Factor Authentication) – A security mechanism requiring users to provide two or more verification factors to gain access to a system or application.

NFRs (Non-Functional Requirements) – Technical requirements that specify system performance, security, availability, and resilience criteria, as distinct from functional requirements that define system behavior.

PCI DSS (Payment Card Industry Data Security Standard) – A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

PEP (Politically Exposed Person) – An individual who is or has been entrusted with a prominent public function, or an immediate family member or close associate of such a person, and who may present a higher risk for money laundering or corruption.

PII (Personally Identifiable Information) – Any information that can be used to identify, contact, or locate a single person, or to identify an individual in context.

PSP (Payment Service Provider) – A licensed third-party entity that facilitates payment transactions between players and the Company.

RBAC (Role-Based Access Control) – A method of restricting system access to authorized users based on their role within the organization.

Recovery Point Objective (RPO) – The maximum acceptable period of data loss measured in time, representing the point in time to which data must be recovered following a failure or disaster.

Recovery Time Objective (RTO) – The maximum acceptable duration of unexpected downtime for a service or system following a failure or disaster.

RNG (Random Number Generator) – A certified software algorithm or physical mechanism used to produce random outcomes in Games of Chance, ensuring fairness and unpredictability.

RTP (Return to Player) – The theoretical percentage of all wagered money that a game will pay back to players over time, expressed as a percentage.

SIEM (Security Information and Event Management) – A platform that provides real-time analysis of security alerts generated by applications and network hardware.

SOC 2 Type II – A report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, and privacy, evaluated over a period of time.

T&Cs (Terms and Conditions) – The general terms and conditions governing the relationship between the Company and its players, as required by Article 5.8(k) and Article 5.9(1)(h) of the National Ordinance on Games of Chance.

TLS (Transport Layer Security) – A cryptographic protocol designed to provide secure communications over a computer network.

UBO (Ultimate Beneficial Owner) – The natural person(s) who ultimately owns or controls the Company, or on whose behalf a transaction is being conducted.

VPC (Virtual Private Cloud) – An isolated virtual network environment within a cloud infrastructure, providing secure and controlled hosting of resources.

Vulnerable Person – A person as defined in Article 1.1(w) of the National Ordinance on Games of Chance, including minors, persons exhibiting problematic gambling behavior, self-excluded persons, and persons who have been declared bankrupt or lack legal capacity to manage their property.

2. SCOPE

2.1 Introduction

This *Operational Manual* (the “Manual”) has been developed under the requirements established by the Curacao Gaming Authority within the scope of the License held by the company. This Manual was developed in accordance with the Article 5.9 of the National Ordinance on Games of Chance (“LOK”). It serves as an official record and reference document demonstrating the Company’s continuous compliance with all provisions, conditions, and restrictions attached to its Gaming License.

2.2 Purpose

The purpose of this Manual is to provide a comprehensive and transparent overview of the Company’s operational framework, ensuring that all gaming activities are conducted in a lawful, secure, and responsible manner. It outlines the structure, processes, and technical measures implemented to safeguard player interests, uphold the integrity of games, and maintain full regulatory compliance.

This document includes detailed information on the Games of Chance offered, payment and betting configurations, software systems, data protection methods, quality assurance procedures, and responsible gaming measures. It also describes the Company’s approach to dispute resolution, technical recovery planning, and the maintenance of digital records as required by the CGA.

The Manual functions as both a compliance tool and an operational guide, ensuring that all employees, management, and related stakeholders adhere to consistent standards of governance, transparency, and accountability. It is maintained as a living document—subject to periodic review and updates—to reflect regulatory developments, technological changes, and continuous improvement in operational practices.

2.3 Amendment Process

Amendments to this Manual may be initiated when:

- Material changes occur to the Company’s operations, technical infrastructure, or gaming offerings;
- New regulatory requirements, CGA guidance, or ministerial regulations are issued;
- Internal audits, risk assessments, or compliance reviews identify necessary updates;
- Deficiencies or inaccuracies in the existing Manual are identified; or
- Annual review procedures require updates to reflect current operational reality.

3. GAMES OF CHANCE

This section is prepared in accordance with Article 5.9(1)(a) of the National Ordinance on Games of Chance, which requires the operations manual to contain a description of the Games of Chance offered as part of the license holder's operations, payment possibilities, bet amounts, payouts, software, and outcome-determining elements. The following subsections provide a comprehensive overview of the Company's gaming portfolio, the payment methods available to players, and the betting parameters applied across the Company's products.

3.1 Description of Games of Chance

The Company offers Games of Chance as part of its licensed operations, defined as games in which the outcome is determined predominantly by an element of chance rather than player skill. All such games are developed, implemented, and operated in accordance with applicable regulatory standards to ensure fairness, integrity, and player protection.

Each Game of Chance operates on certified software using approved random number generators (RNGs) or, where applicable, physical randomization mechanisms. The RNGs and game systems are independently tested and certified by CGA approved laboratories to verify randomness, reliability, and compliance with technical and regulatory requirements.

The portfolio of Games of Chance may include slot games, table games, live dealer games, instant win and lottery-style games, and betting on real or simulated events. For each game, the Company maintains comprehensive documentation describing its functionality, rules, payout structure, and theoretical return to player (RTP). Such documentation is reviewed and updated as required to reflect software changes, regulatory updates, or operational adjustments.

All games specify applicable bet limits and payout parameters in accordance with responsible gaming principles. These limits are established to ensure fair play and prevent excessive gambling behavior. The Company ensures that all game outcomes are determined solely by certified systems and that no manual or external interference can affect the result.

The software used in connection with the Games of Chance is supplied exclusively by licensed and reputable providers, and its deployment is subject to prior approval by the Compliance and Technical Departments. Both departments are responsible for maintaining records of certifications, software versions, payout configurations, and testing results, and for ensuring continuous monitoring of system integrity and performance.

The Company's approach to game design and operation emphasizes regulatory compliance, technical transparency, and the protection of players' interests. All activities related to the offering and operation of Games of Chance are documented and available for inspection by the relevant authorities upon request.

3.2 Payment Methods

The Company provides players with access to a broad range of secure and compliant payment methods, ensuring flexibility and convenience across multiple jurisdictions. All payment systems integrated into the Company's platform are verified for compliance with applicable financial, anti-money laundering (AML), and data protection regulations.

Accepted payment methods include card payments, bank transfers, e-wallets, carrier billing, cash-based solutions, pass-through wallets, and cryptocurrency transactions. Each method is supported through licensed and reputable payment service providers (PSPs), and all transactions are processed through secure and encrypted channels.

Card payments include major international card schemes such as Visa and Mastercard, as well as other globally recognized networks including American Express (Amex), JCB, and UnionPay. Local card schemes may also be supported depending on the player's region of residence. Bank transfers are facilitated through online or mobile banking channels and are authorized directly by the player. Depending on the jurisdiction and banking infrastructure, transfers may be processed either in real time via instant interbank payment systems or within standard banking timeframes.

E-wallets allow players to fund their accounts using virtual wallets linked to bank accounts or cards. The Company accepts widely used e-wallets such as PayPal, Skrill, Neteller, and AstroPay. These solutions enable fast deposits and withdrawals while maintaining high standards of security and transaction traceability.

Carrier billing is available in selected regions, enabling players to deposit funds directly from their mobile phone accounts. Payments are authorized through secure SMS or IVR verification processes in cooperation with licensed telecom operators.

Cash-based payment methods are provided for players without access to banking services. These include physical payment terminals and authorized intermediaries that accept cash deposits on behalf of the Company. Upon confirmation of the payment, the corresponding amount is credited to the player's gaming account. Pass-through wallets, including Apple Pay and Google Pay, allow transactions to be processed through linked payment instruments without maintaining stored balances. These systems enhance data security by minimizing the disclosure of sensitive financial information.

The Company also supports cryptocurrency payments, recognizing their relevance within the iGaming sector. When a player selects a cryptocurrency deposit option, the Payment Gateway generates a unique transaction identifier or merchant wallet address to ensure accurate linkage between the player's deposit and account. All cryptocurrency transactions are processed in accordance with the Company's AML and transaction monitoring framework.

The Compliance and Finance Departments are jointly responsible for maintaining a current registry of all approved payment methods and providers, ensuring that every integration meets the Company's operational, technical, and regulatory requirements.

3.3 Bet Settings and Parameters

The Company establishes and maintains standardized bet configuration parameters to ensure fair, consistent, and responsible betting practices across all products offered under its license. All bet limits and related parameters are defined in accordance with regulatory requirements, internal risk management policies, and platform capabilities.

The configuration of base betting parameters includes the definition of minimum bet amounts, maximum odds, maximum payouts, default bet amounts, and preset bet amounts. These settings are established for all game types and betting formats, including single bets, parlay bets, and system bets.

The minimum bet amount defines the lowest permissible wager that a player may place and is established separately for single, parlay, and system bets. The minimum bet must always exceed zero and is expressed in the operational currency assigned to the respective brand.

The maximum odds parameter limits the highest odds value that may be accepted in a player's betslip, ensuring that betting remains within a controlled and transparent framework.

The maximum payout represents the upper limit of potential winnings payable per bet. This measure serves as a financial safeguard against exposure to disproportionate risks arising from unforeseen outcomes. The value is determined and approved by the Company in alignment with its risk and liability management policies.

The default bet amount specifies the pre-filled wager value displayed to the player when adding a selection to their betslip. This configuration simplifies the betting process and ensures consistent presentation of bet amounts.

The preset bet amounts provide players with predefined wager options that can be selected instantly. The preset amounts include several standardized values as well as the maximum permissible bet per event. Each preset must comply with established minimum and maximum thresholds and be denominated in the operational currency of the brand.

All bet configurations are reviewed and approved by the Company's Risk Management and Compliance Departments prior to implementation. Any adjustments to limits, odds, or payout parameters must be documented, authorized, and verified to ensure alignment with the Company's internal controls and responsible gaming framework.

4. SYSTEM TESTING AND ACCEPTANCE

Addressing the requirement of Article 5.9(1)(b) of the National Ordinance on Games of Chance, this section describes the periodically used test methods for quality monitoring applied by the Company, including its approach to system testing, acceptance criteria, and ongoing quality assurance procedures designed to ensure the continued reliability, security, and integrity of all software systems, platforms, and integrated components supporting the Company's gaming operations.

The Company ensures that all software systems, platforms, and integrated components undergo comprehensive testing and validation prior to deployment in the production environment. All remote Games of Chance, whether developed in-house or supplied by third-party providers, are certified for soundness and integrity by independent testing laboratories approved by the CGA (Gaming Laboratories International LLC GLI, eCOGRA Limited, Quinel Limited, BMM Spain Testlabs S.L.U.). The objective of this process is to confirm the reliability, security, and regulatory compliance of all technological solutions supporting gaming operations.

Acceptance criteria shall be formally defined for each software component and integrated system to ensure that all security, functionality, and performance requirements are met. Test cases are developed and maintained to verify the proper implementation of security controls and operational safeguards.

No software, system update, or configuration change may be introduced into the production environment without successful completion of acceptance testing. Testing must be conducted across all relevant operational scenarios to validate performance under normal and exceptional conditions.

A structured test procedure is implemented to govern all testing activities, including issue identification, escalation, and resolution. All identified defects or deviations must be recorded, assessed for impact, and resolved prior to production deployment. Any unresolved critical issues shall trigger a formal escalation to the responsible technical and compliance teams.

4.1 Protection of System Test Data

The Company applies strict controls to ensure the protection of all data used in testing environments. Operational data containing personal information or real business values shall not be used for testing purposes unless properly de-personalized or replaced with fictional equivalents through hashing or anonymization techniques.

If the use of operational data is deemed necessary, the data must undergo de-personalization prior to import into any test environment. Under no circumstances may de-personalized data be transferred outside of the testing environment or reintroduced into production systems.

All data handling within testing processes must comply with applicable privacy and data protection legislation, including but not limited to the principles of lawful processing, purpose limitation, and data minimization.

In cases where technical de-personalization is not feasible, the Company shall initiate a formal risk acceptance procedure, ensuring that the residual risk is documented, justified, and approved by the appropriate level of management.

The Information Security Department is responsible for oversight of system testing, approval of acceptance criteria, and enforcement of data protection measures within all testing environments.

5. THE WAY OF STORING PLAYERS' PERSONAL DATA AND OTHER DETAILS

In fulfilment of the obligation set out in Article 5.9(1)(c) of the National Ordinance on Games of Chance, this section sets out the Company's framework for storing players' personal data and other details. It covers the regulatory basis for the Company's data processing activities, the technical infrastructure used for data storage, the categories of personal data collected and the applicable retention periods, the security standards and access controls in place, the mechanisms for providing regulatory access to the CGA, and the governance arrangements overseeing the Company's data protection practices.

5.1. Regulatory Requirements

The Company maintains a digital registration of all critical player personal data, gaming transactions, and financial transactions in accordance with the National Ordinance on Games of Chance, Curaçao Gaming Authority (CGA) regulations, the National Ordinance Personal Data Protection, and where applicable, the General Data Protection Regulation (GDPR).

5.2. Data Storage Infrastructure

The Company employs Amazon Web Services (AWS) as its principal data storage and processing infrastructure. AWS provides a highly secure, resilient, and scalable cloud environment that meets or exceeds the security, availability, and integrity standards associated with Tier IV data centers. All operational systems, player data, and transactional records are hosted within AWS under strict security and access-control protocols, ensuring compliance with international information-security and data-protection requirements.

In alignment with the National Ordinance on Games of Chance and related regulatory obligations, the Company will also utilize a Tier IV-certified data center located in Curaçao to supplement its existing AWS infrastructure. This facility will be employed for the storage of specific categories of critical information and for other functions expressly prescribed by the applicable regulations.

To ensure both compliance and continuity, selected datasets will be securely synchronized and mirrored between AWS and the Curaçao-based data center using encrypted data transfer protocols and controlled replication mechanisms. This hybrid hosting approach allows the Company to maintain high operational performance, redundancy, and data integrity while meeting all jurisdictional requirements for data localization and regulatory oversight.

5.3. Categories of Personal Data and Retention Periods

The Company stores the following categories of data:

a) Identity Data: Full name, date of birth, password (encrypted), identification number, and unique user ID.

b) Contact Data: Email address and phone number.

c) KYC Data: Identity verification documents (ID card, passport, driver's license, photo), source of funds documentation (bank statements, tax returns, payslips), proof of address (utility bills), politically exposed person (PEP) status and relevant details, international sanctions data, and ultimate beneficial owner (UBO) information. Additional information may be collected for identity verification, anti-money laundering (AML), Know-Your-Customer (KYC) checks, and affordability assessments.

d) Communication Data: Records of calls, texts, and other communications, including date and time of communications, content of communications, and responses to Company communications.

e) Financial Data: Bank account details, alternative payment methods, limited payment card details (e.g., last four digits), transaction records including deposits and withdrawals, payment amounts, and payer identity.

f) Gaming Data: Gaming activity information including bet amount, currency, date and time of bet, game play history, game outcomes, RNG data, and bonus information.

g) Marketing Data: Marketing permissions, responses to marketing activities (campaigns, competitions, offers), and interaction data with marketing communications.

h) Profile Data: Information based on profiling activity derived from any personal data held, used for compliance with legal and regulatory obligations, risk analysis, and tailored product offerings.

i) Technical Data: Device hardware and software information, browser details, time and date of access, IP address, and geolocation data (country, city, internet service provider).

j) Usage Data: Website usage information including pages visited, content viewed, links and buttons clicked, and navigation patterns.

The Company retains personal data only as long as necessary for the purposes collected, balanced against legal obligations:

- Identity Data, Contact Data, and KYC Data: Duration of account activity plus 5 years following account closure.
- Gaming Data: Minimum 5 years from transaction date.
- Financial Data: Minimum 7 years from transaction date.
- Communication Data, Marketing Data, Profile Data: Duration of account activity plus 5 years following account closure.
- Technical Data and Usage Data: Retained for operational and security purposes during the account activity period.
- Compliance and AML records: Minimum 7 years from account creation date.

These retention periods comply with Curaçao's AML/CFT requirements under National Ordinance on the Reporting of Unusual Transactions and National Ordinance on Identification when Rendering Services. Where retention periods exceed regulatory minimums (financial and compliance records retained for 7 years), this reflects the Company's commitment to robust compliance, international best practices, and the protection of both player and business interests.

5.4. Security Standards

The Company's hosting provider AWS maintains ISO/IEC 27001:2022, ISO/IEC 27701:2019, SOC 2 Type II, PCI DSS Level 1, ISO/IEC 27017:2015, and ISO/IEC 27018:2019 certifications.

Data Protection Measures:

- Encryption: TLS 1.3 for data in transit; AES-256 with automated key rotation for data at rest.
- Access Controls: Role-based access control (RBAC), multi-factor authentication (MFA), comprehensive access logging, and periodic access reviews.
- Network Security: VPC isolation, network segmentation, firewall rules, intrusion detection/prevention systems, DDoS protection, and ongoing vulnerability management.
- Monitoring: 24/7 security monitoring, automated anomaly detection, SIEM platform, and documented incident response procedures.
- Backup and Recovery: Detailed backup procedures, retention schedules, and disaster recovery protocols are described in Section 11 (Backup Plan) of this Manual.

5.5. Data Protection Compliance

Lawful Basis for Processing:

The Company processes player data under contract performance (service delivery), legal obligation (regulatory compliance, AML/KYC, responsible gaming), and legitimate interests (fraud prevention, security, business analytics).

The Company adheres to the principle of transparency by clearly communicating the purposes and lawful bases for data processing in its Privacy Notices to players.

Player Rights:

The Company facilitates the exercise of player rights including access, rectification, erasure (subject to legal retention obligations), restriction of processing, data portability, and objection to processing. All requests are processed within statutory timeframes as outlined in the Company's Privacy Notices constantly available to players.

6. VISUAL REPRESENTATION OF PLAYER INTERFACE ELEMENTS

This section presents the visual elements displayed to players through the Company's gaming website and software applications, in accordance with Article 5.9(1)(d) of the National Ordinance on Games of Chance. The screenshots and descriptions below depict the platform interface in its pre-product state, without brand specific personalisation applied.

All products within the Company's portfolio operate on a shared platform architecture: while individual brands may differ in logo, colour scheme, and other design elements, the underlying website mechanics, navigation structure, and player-facing functionality remain consistent across all products. Accordingly, the interface elements illustrated in this section are representative of the player experience across the Company's full range of licensed operations.

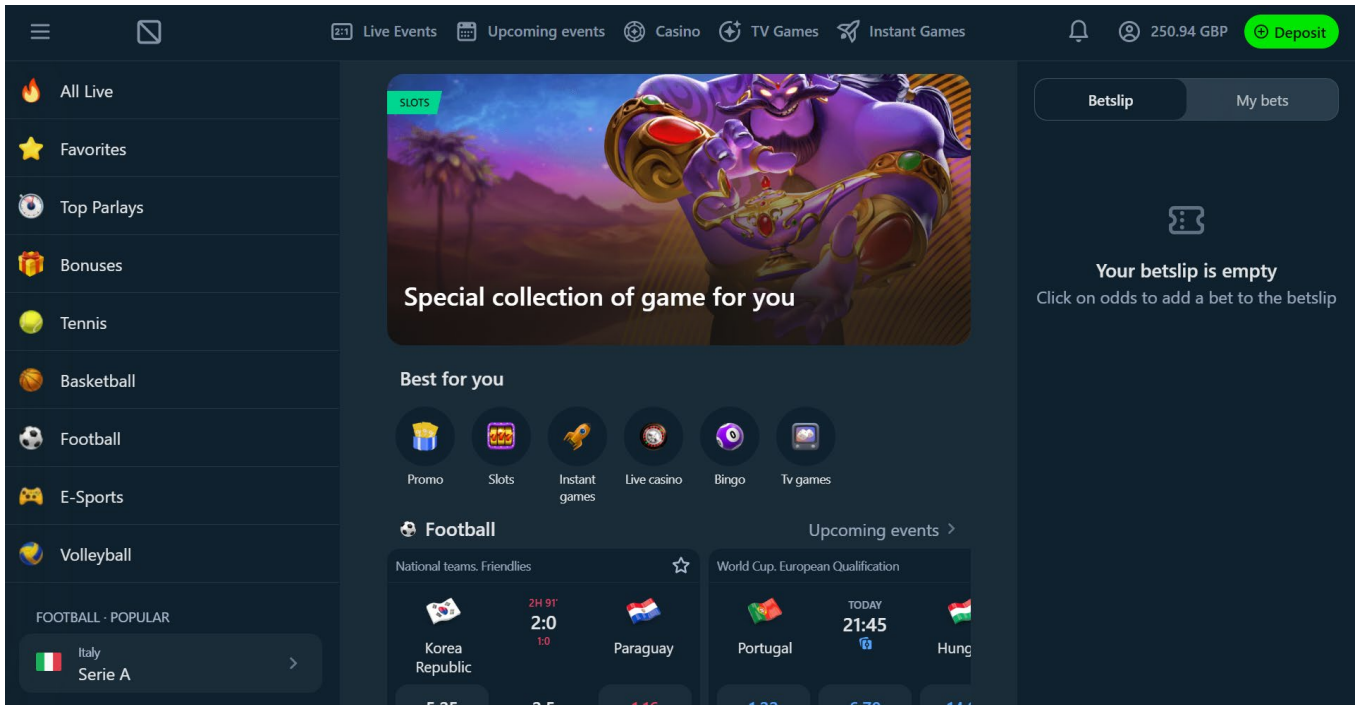
The platform used by the Company for its products has recently undergone a significant upgrade to achieve full alignment with the requirements of the National Ordinance on Games of Chance and the conditions attached to the Company's Gaming License. The current version of the platform provides players with a comprehensive, intuitive, and secure environment for online entertainment.

All player-facing interfaces are designed to ensure ease of navigation, transparency of gaming and financial information, and continuous access to responsible gaming tools, support services, and regulatory disclosures. The Company is committed to the ongoing development and refinement of the platform to maintain compliance with evolving regulatory standards while delivering a reliable and enjoyable player experience.

6.1 Home page or Lobby

Lobby. The Lobby serves as the main homepage interface displaying featured games, promotions, and navigation shortcuts, allowing players to access all gaming categories and account functions from a centralized dashboard.

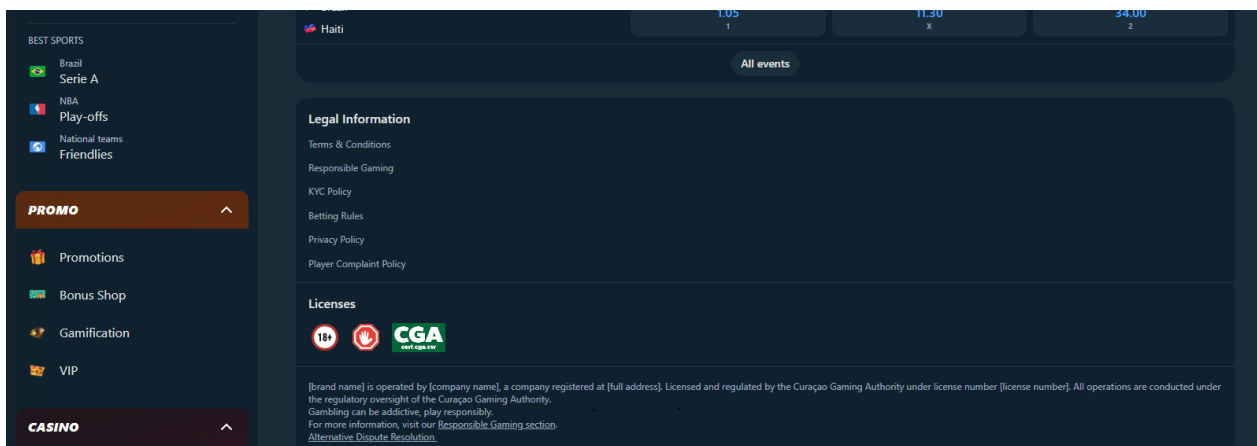
Lobby provides players with access to all the gaming / betting modules with respective submodules, Player's account menu and various policies and information available to the player.



At the bottom of the Lobby page, the player has access to various subpages containing relevant information about gaming and betting rules, as well as the policies governing the operation of the website. Among the published policies are those required to be made available to the player under CGA regulations, including:

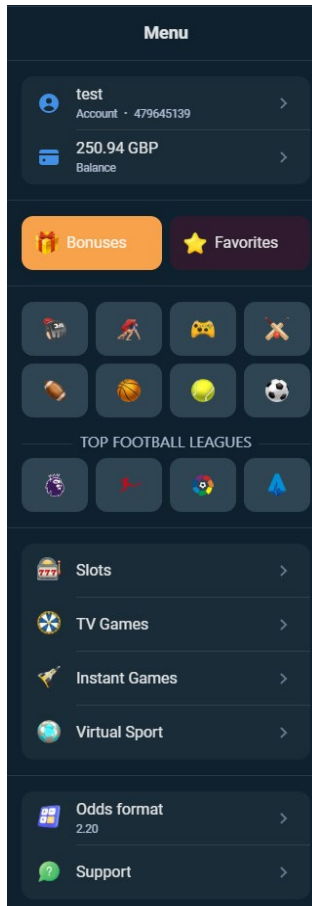
- Terms and Conditions;
- Responsible Gaming Policy;
- AML and KYC Policies;
- Dispute Resolution Policy.

The footer also contains other mandatory information, including the legal details of the license holder, a notification regarding the Company's CGA license status, a dynamic CGA license seal, and responsible gaming notifications.



6.2 Side menu

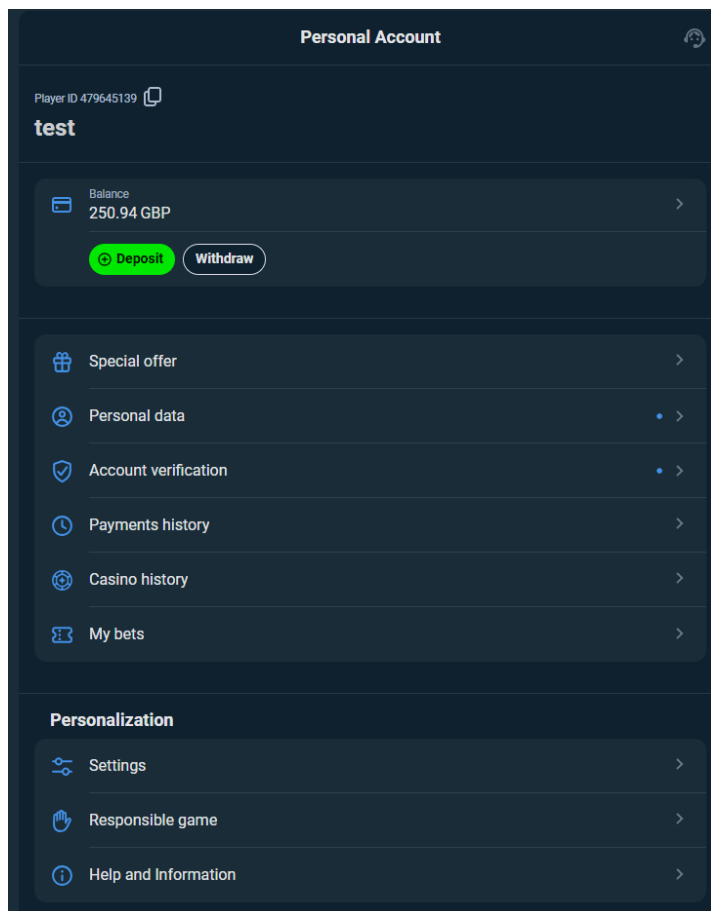
The Side Menu provides persistent navigation throughout the platform, offering quick access to player account, basic settings (language, odds format) support services, and all major gaming categories.



6.3 Player account menu

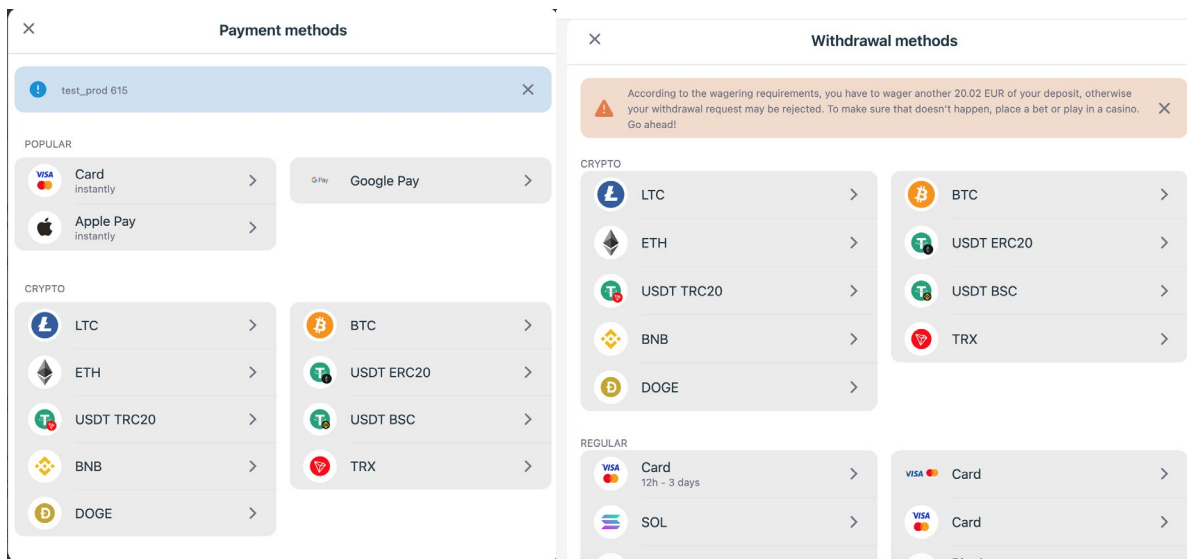
Personal account menu provides access for players to different modules including:

- Payment module for depositing and withdrawal of funds
- Personal offer section
- Personal data management
- Verification module for the purpose of AML checks
- Transaction, casino and betting history
- Account settings
- Responsible gaming features



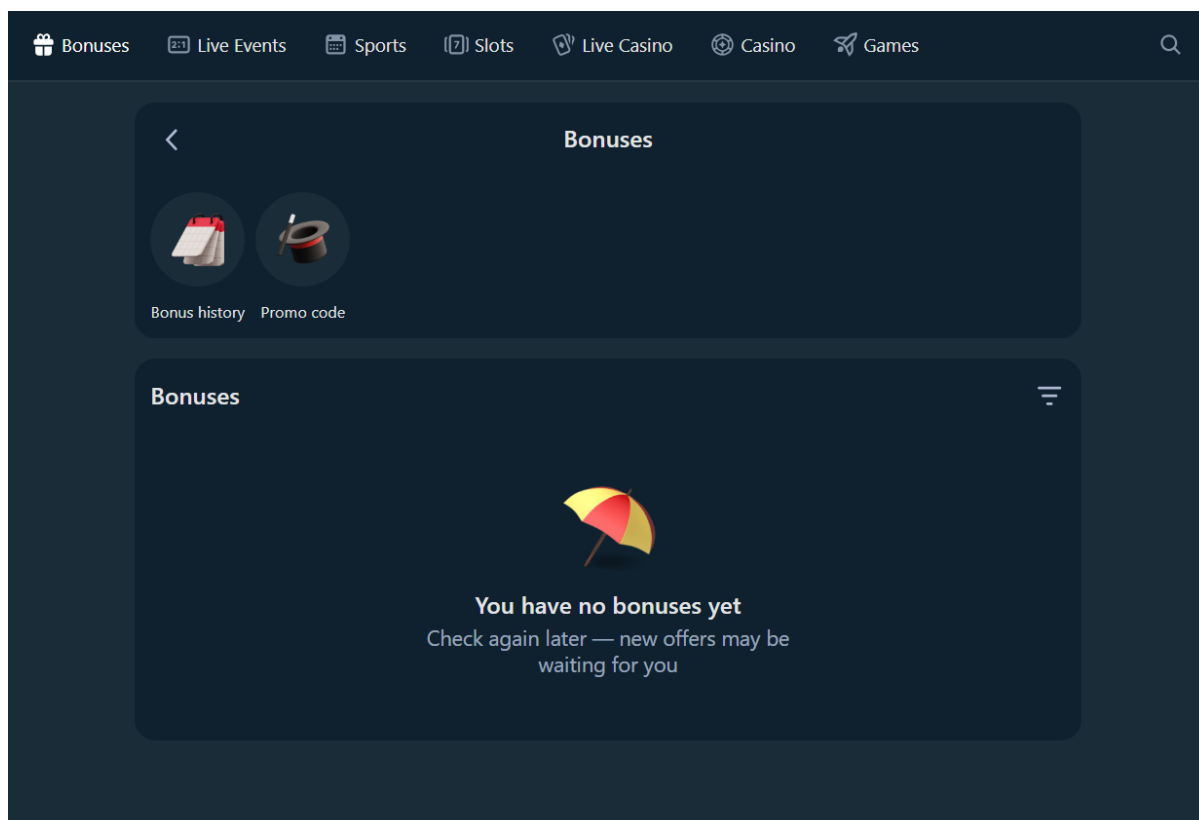
6.3.1. Payment module for depositing and withdrawal of funds

Payment module provides for various options for money depositing and withdrawal that are enabled on a brand. The transactions are processed on a semi-automated way: subject to a platform restriction (i.e. based on personal limits and thresholds) or manual review can be triggered if transaction is classified as unusual / suspicious or high risk.



6.3.2. Special Offer (Bonuses)

This section displays all promotional offers, bonus credits, and loyalty programme benefits associated with the players account.



6.3.3. Personal data management

This module enables players to view and modify registered account information, including full name, email address, contact telephone number, date of birth, and address.

The screenshot shows a mobile application interface for managing personal data. At the top, there is a navigation bar with icons and labels for 'Bonuses', 'Live Events', 'Sports', 'Slots', 'Live Casino', 'Casino', and 'Games'. Below this, the main screen is titled 'Personal data' with a back arrow on the left and a help icon on the right. The interface is divided into several sections: 1. 'Confirm contacts': A message with a red exclamation mark icon asking the user to confirm their contacts. 2. 'CONTACTS': A section containing three rows of contact information: 'Account number' (766750884) with a copy icon, 'Phone number confirmed' (+56994****00), and 'E-mail (not confirmed)' (test12333@gmail.com). A blue 'Confirm' button is located at the bottom of this section. 3. 'PERSONAL INFORMATION': A section with five rows of personal details: 'First Name' (Test), 'Last Name' (Test), 'Date of birth' (06.11.1990), and 'Country' (Chile). Each row has an edit icon (pencil) on the right. 4. 'ADD YOUR DETAILS': A section with three input fields: 'City', 'Secret question' (with a 'PIN code (...)' dropdown), and 'Secret answer'. A large 'Save' button is positioned below these fields. 5. A footer section with an information icon and the text 'Problems with personal data? Contact support'.

Personal data

Confirm contacts
Please confirm your contacts so you can play to the fullest

CONTACTS

Account number
766750884

Phone number confirmed
+56994****00

E-mail (not confirmed)
test12333@gmail.com

Confirm

PERSONAL INFORMATION

First Name
Test

Last Name
Test

Date of birth
06.11.1990

Country
Chile

ADD YOUR DETAILS

City

Secret question PIN code (...)

Secret answer

Save

Problems with personal data? Contact support

6.3.4. Verification module for the purpose of AML checks

The Verification module allows users to upload the required KYC documents to be further processed for verification of the personal data provided in a Player's profile above. Players must submit mandatory documentation including government-issued identification and driving license or other proof of residence to complete the Know Your Customer (KYC) process and enable unrestricted withdrawal privileges. The review is semi-automated with manual review triggered for unclear / high risk cases.

< 



Verify identity

Choose one of the fast verification methods or
upload the documents yourself

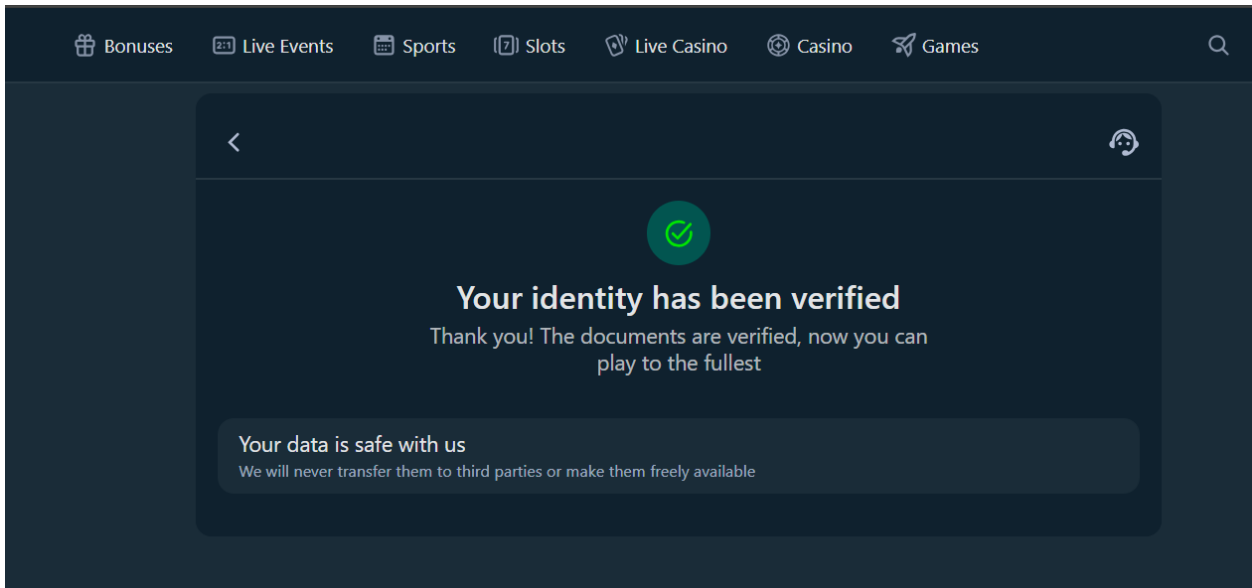
UPLOADING DOCUMENTS

 Passport >

 Driver's license >

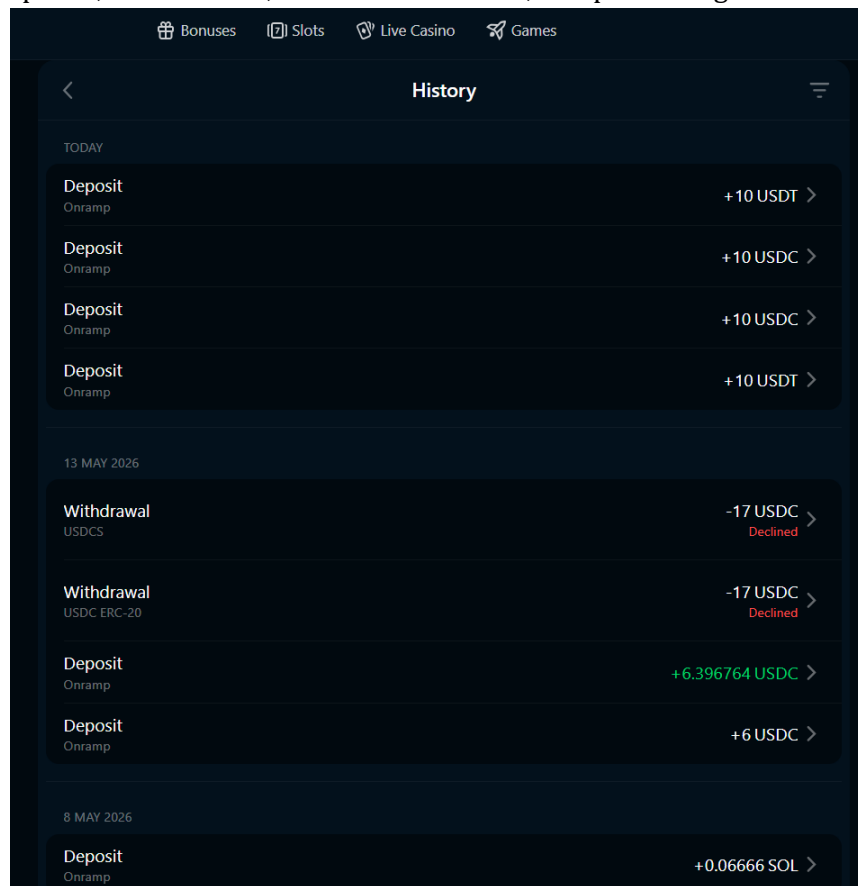
Your data is safe with us
We will never transfer them to third parties or make them freely available

Once the validation is completed, the players receive the appropriate confirmation. If the Personal data is changed, the verification requirement can arise again to validate the amended information (i.e. change of residential address).



6.3.5. Transaction history

This module provides a comprehensive record of all financial transactions associated with the account, including deposits, withdrawals, account corrections, and processing statuses.



6.3.6. Casino history

This section maintains a complete audit trail of all casino gaming activity, including game title, session duration, stake amounts, payout values, and net result per session.

Bonuses

Slots

Live Casino

Games

<

Casino history

1 APRIL 2026, 09:49

Instant Games Winnings

Total Balance

Game: Aviator

+0.52 USDT

41.232269 USDT

>

Instant Games Bet

Total Balance

Game: Aviator

-0.5 USDT

40.712269 USDT

>

Instant Games Winnings

Total Balance

Game: Aviator

+0.52 USDT

41.212269 USDT

>

Instant Games Bet

Total Balance

Game: Aviator

-0.5 USDT

40.692269 USDT

>

Instant Games Winnings

Total Balance

Game: Aviator

+0.52 USDT

41.192269 USDT

>

1 APRIL 2026, 09:48

Instant Games Bet

Total Balance

Game: Aviator

-0.5 USDT

40.672269 USDT

>

Instant Games Winnings

Total Balance

Game: Aviator

+0.52 USDT

41.172269 USDT

>

6.3.7. Betting history

The Bets Menu displays the player's betting activity including open bets, settled bets, and bet history, showing bet details, settlement status, and transaction timestamps to ensure full transparency and enable players to monitor their gambling behavior.

Open

Settled

Nº2 · Feb 6, 09:19

 Full-time result
Arsenal FC

1.23 >

FEB 7, 17:00

Arsenal FC

3

Sunderland

0

Bet amount

1.00 USDT

Cashed out

1.00 USDT

 Share bet

Nº1 · Feb 6, 09:19

 Full-time result
Arsenal FC

1.23 >

FEB 7, 17:00

Arsenal FC

3

Sunderland

0

Bet amount

1.00 USDT

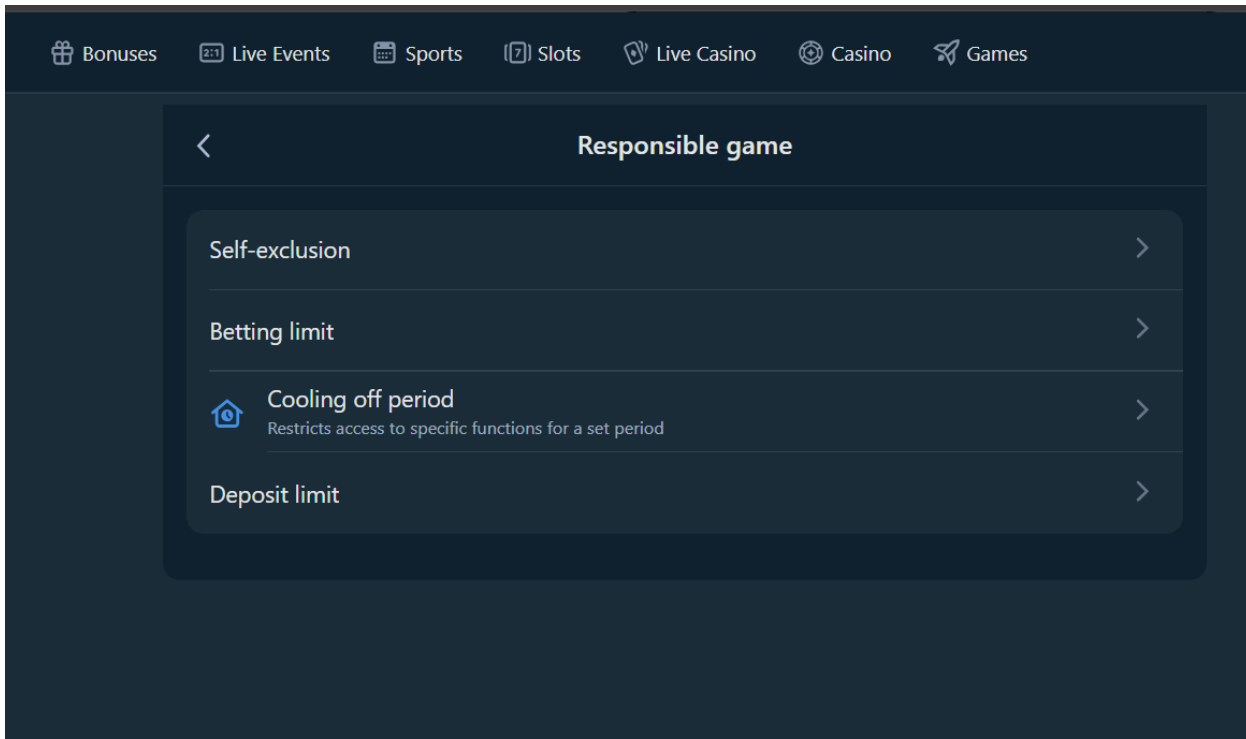
Cashed out

1.00 USDT

 Share bet

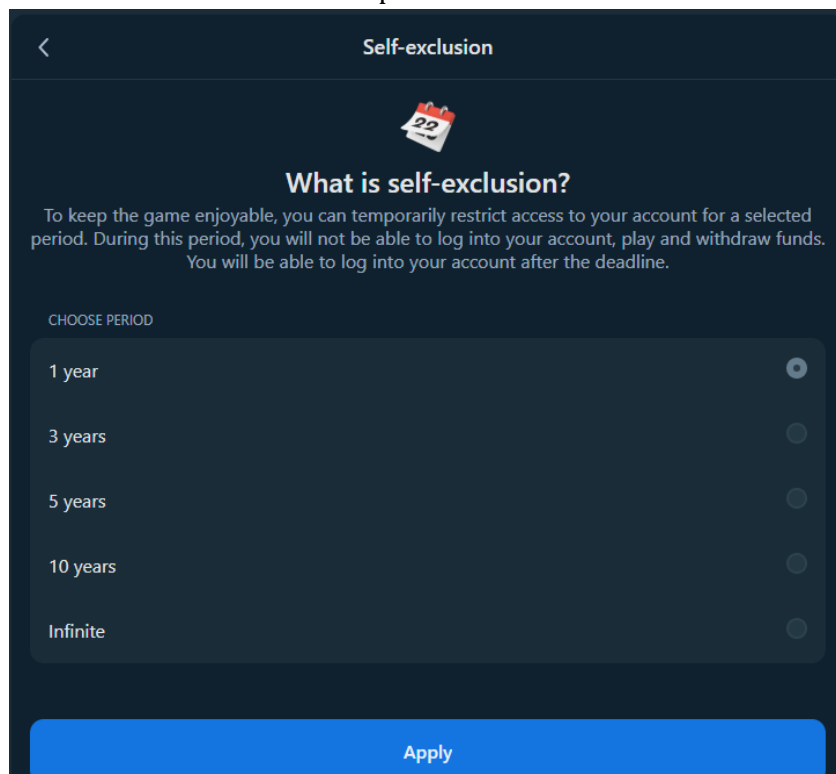
6.3.8. Responsible gaming module

The Responsible Game section provides dedicated access to player protection tools including self-exclusion, betting limits, cooling off and deposit limits options.



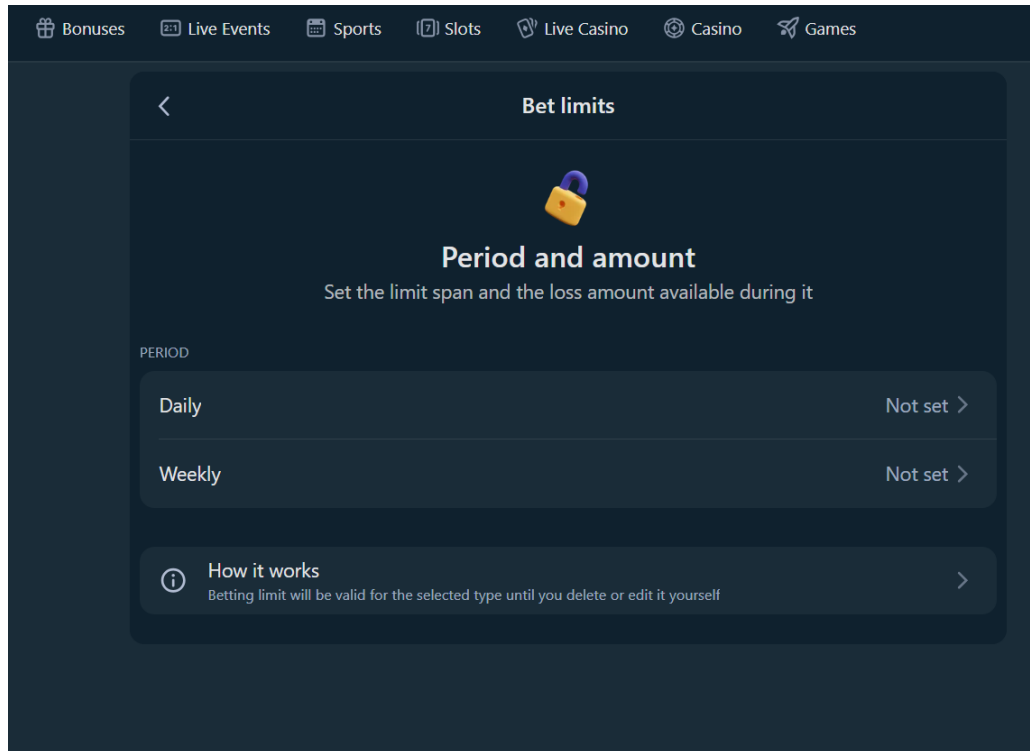
6.3.8. (a) Self Exclusion

This function enables users to voluntarily suspend account access for a predetermined period ranging from one year to permanent closure. Upon activation, all account functionality is immediately disabled, preventing deposits, wagering, and account access for the duration of the self-exclusion period, which cannot be reversed or shortened once implemented.



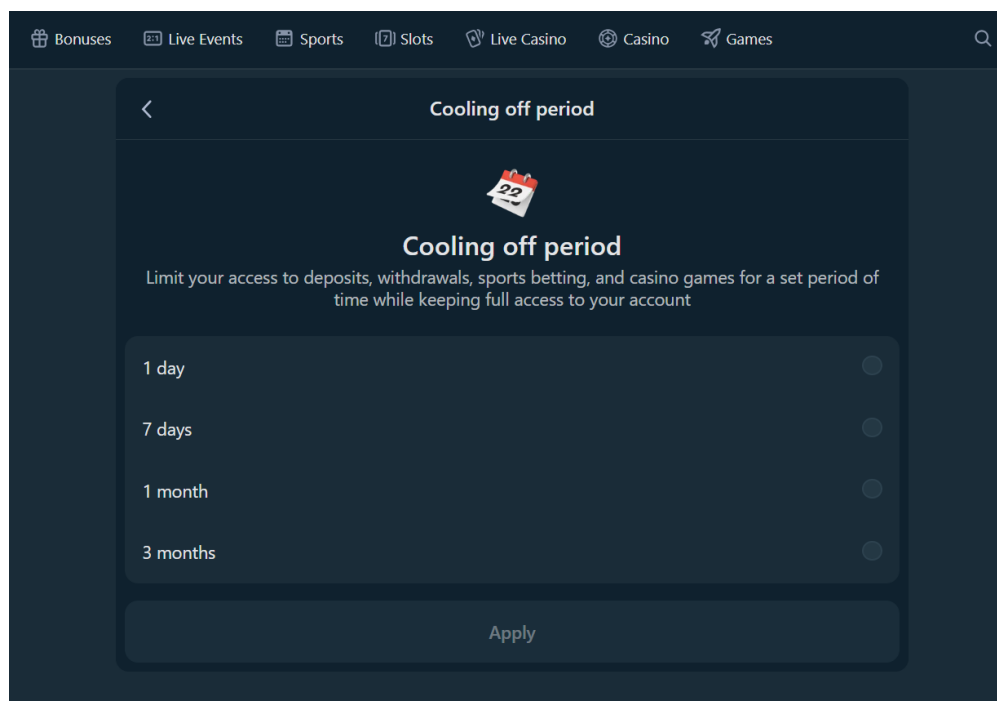
6.3.8. (b) Betting Limit

The amount of the total betting limit applies to Casino and Sports. Once the limit is reached the possibility to place a bet or wager is restricted until the limit timer restarted.



6.3.8. (c) Cooling Off

This temporary account suspension mechanism allows users to take a short-term break from gambling activity, typically ranging from 24 hours to 3 months. During the cooling-off period, account access is open but can gambling activity is stopped.



6.3.8. (d) Deposit limit

This control allows players to establish maximum deposit thresholds on a daily, weekly, or monthly basis to manage expenditure responsibly. Once configured, the system will automatically restrict any deposit transaction that would exceed the specified limit.

<

Deposit limits



Period and amount

Set the limit span and amount available for deposit during it

PERIOD

Daily

Not set >

Weekly

Not set >

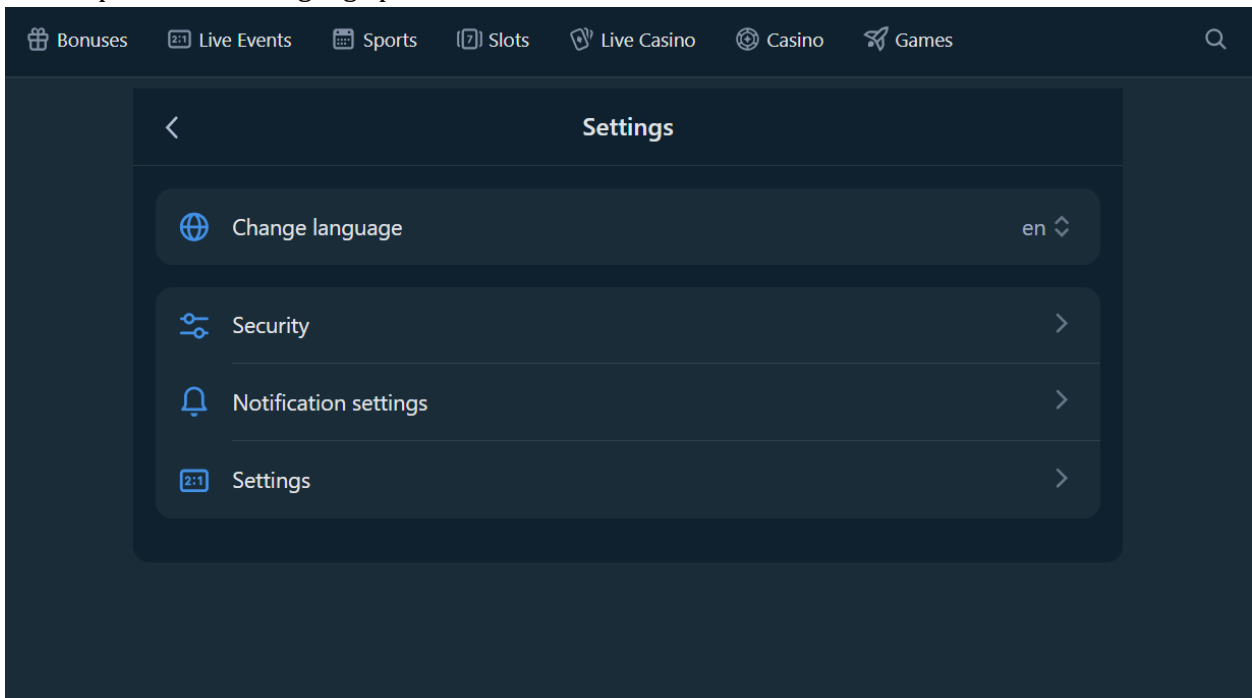


How it works

You can set daily, weekly, or monthly limits. The limit will be applied once you've reached any of the limits within the specified period.

6.3.9. Account settings

This section provides access to account configuration options, including password management, notification preferences, language preferences.



7. TECHNICAL INFRASTRUCTURE AND DISASTER RECOVERY PLAN

This section of Manual addresses the requirements pursuant to Article 5.9(1)(f) of the National Ordinance on Games of Chance and provides a diagram of the Company's technical infrastructure together with a description of the restoration possibilities in the event of a technical emergency situation arising in relation to the Company's operations. It sets out the Company's non-functional requirements for service resilience, backup and recovery standards, high availability architecture, data criticality classifications, periodic restoration testing procedures, and monitoring and response protocols. The section concludes with a diagram of the Company's technical infrastructure, illustrating the key components, data flows, and interdependencies that support the Company's gaming operations.

7.1 Non-Functional Requirements (NFRs) for Every Service

Each service must define and document specific Backup and Recovery as well as High Availability (HA) requirements as part of its Non-Functional Requirements (NFRs). These requirements must be explicitly outlined and implemented to ensure business continuity and resilience. The following information must be explicitly included as part of the NFRs to ensure the product aligns with the company's data protection and business continuity policies:

1. Criticality of the service.
2. Backup and Recovery Requirements.
3. High Availability (HA) Requirements.

The Head of Engineering **MUST** approve the described requirements, and the requirements **MUST** be implemented before deploying the service to production.

7.1.1 Backup and Recovery Plan Requirements

The definition of the Backup and Recovery plan must be explicitly included as part of the NFRs to ensure the product aligns with the company's data protection and business continuity policies. The Backup plan must reveal all Data Types that should be backed up (databases, logs, media files, configurations, etc.). For each Data Type, there **MUST** be described the next information:

Backup Strategy

- Backup frequency and schedule.
- Retention period - Define how long backups are stored.
- Backup redundancy - Specify whether backups are stored across multiple locations or regions.

- Storage Information - Include the storage type (e.g., database, virtual machine, object storage) and physical locations.

Recovery Objectives:

- Recovery Time Objective (RTO): Maximum allowable downtime for the service.
- Recovery Point Objective (RPO): Maximum allowable data loss.

Restoration Process

- Step-by-step recovery procedures.
- Testing and validation of data integrity (if applicable) to confirm that data was successfully restored.
- Roles and responsibilities in the recovery process.

7.1.2 High Availability (HA) Requirements

To complement backup and recovery measures, high availability (HA) requirements must be defined and implemented to prevent service disruptions. They should be described both for service and database and should cover the following:

Redundancy & Failover Mechanisms.

- Load Balancing Strategy
- Autoscaling Strategy or other HA configuration
- Data Redundancy strategy (Replication, Sharding, or other strategies + description of a Failover Mechanism)

Geographical Distribution.

- Multi-zone or multi-region failover strategy.
- Latency Requirements for multi-zone or multi-region replications.

Automated Monitoring & Self-Healing.

- Proactive monitoring and alerting mechanisms.
- Automated recovery procedures for service failures.

7.1.3 Data Criticality Definitions

Backup plans **MUST** include requirements that align with the standards outlined in this document, tailored appropriately based on the criticality level of the service and data that it contains:

High

Service and data whose unavailability or loss would cause the **entire Platform** to stop functioning, lead to severe financial loss, reputational damage, or violate legal/compliance requirements.

Examples:

- Centralized user authentication systems (e.g., user credentials, access permissions).
- Personally Identifiable Information (PII) or data subject to strict compliance standards (e.g., GDPR, HIPAA).
- Critical information for the Platform's operability (balances, critical configurations, etc.)
- Anti-fraud information (e.g. restrictions and limitations)

Minimum Requirements:

- Backup Retention: 1 week and frequent point-in-time recovery options.
- Backup Frequency: Daily full backups.
- Backup Locations: At least 2 different Data Centers for backups (multi-region backup storage should be preferred for critical data).
- RTO: Maximum 20 minutes to restore operations.
- RPO: Near-zero data loss.
- HA requirements: Real-time or near-real-time replication in at least 3 different Data Centers with automatic switching to a working replica in case of failure.

Medium

Service and data whose unavailability or loss would impact a **specific product** (Casino, Sport, CRM, etc) within the platform or **specific product major features**, leading to degraded functionality or loss of service for that product. It could impact the operational work of b2b clients (operators) or could also lead to high financial loss and reputational damage.

Examples:

- Product-specific databases (e.g., player bonuses, sports bets).
- Feature settings or configurations critical to the product's operation (e.g. player segments, recommendations data, etc.).

Minimum Requirements:

- Backup Retention: 1 week and frequent point-in-time recovery options.
- Frequency: Daily full backups.
- Locations: At least 2 different locations for backups (multi-zone is enough)
- RTO: Within 1 hour.
- RPO: Up to 1 hour of potential data loss.
- HA requirements: Real-time or near-real-time replication in at least 3 different Data Centers with automatic switching to a working replica in case of failure.

Low

Service and data whose unavailability or loss would affect **specific product non-major features**, causing inconvenience to users but not full operational failure. It could also affect the internal operational work or investigation of issues.

Examples:

- Player UI configurations (if there exists a fall-back configuration or a long-term cache that will be used instead of the unavailable data)
- Some technical metrics or service logs.

Minimum Requirements:

- Retention: 1 week
- Frequency: 2 times a week full backups, with incremental backups as needed (e.g., every 12–24 hours).
- Locations: At least 1 location different from the original data source.
- RTO: Within 6 hours.
- RPO: Up to 24 hours of potential data loss is acceptable.

Non-Critical

Data and services whose unavailability or loss would not impact the operation of the platform, products, or features, and whose loss poses minimal financial or reputational risk.

- Archived logs are no longer actively used for compliance or analytics.
- Technical logs of non-critical services.

Requirements:

- Retention, Frequency, Locations, RTO, RPO, HA: up to the team (must be approved by the Head of Engineering by considering costs).

7.1.4 Briefly described requirements depending on the data criticality

	Data criticality	High	Medium	Low	Non-Critical
Minimum requirements	Backup min schedule	daily	daily	2 times a week	As needed
	Backup min availability	1 week	1 week	1 week	As needed
	Backup min locations	2 storages	2 storages	1 storage	As needed
	RTO	20 minutes	1 hour	6 hours	As needed
	RPO	Near real-time	1 hour	24 hours	As needed
	HA	Real-time or near-real-time	Real-time or near-real-time	As needed	As needed

		application in at least two different DCs with automatic switching to a working replica in case of failure.	application in at least 3 different DCs with automatic switching to a working replica in case of failure.		
--	--	---	---	--	--

7.1.5 Separated Locations Requirement

When implementing the Disaster recovery or HA requirements the following criteria must be satisfied for different Data Centers:

- The Data Centre storage facility shall either have an alternate source of backup power or be on a different power grid than the Group facility;
- Each Data Centre has either independent emergency fail-over power supplies or is on different power grids;
- The storage must be equipped with a redundant disk array.

As an alternative, use cloud storage.

7.2 Periodical Data Restoration Testing

Teams responsible for High and Medium critical services **MUST** conduct periodic restoration tests to verify backup integrity and ensure disaster recovery readiness.

The purpose of this test is to proactively identify and address any potential issues that could impact data recovery. Each restoration attempt **MUST** be fully documented, including any errors or inconsistencies. Maintaining these logs helps to:

- Identify trends and recurring issues.
- Provide a record of successful restorations.
- Build confidence in the overall backup and restoration process.

Another key benefit of regular restoration tests is that they familiarize teams with the recovery process, ensuring that they can efficiently restore data storage and services in a real failure scenario.

Any unsuccessful backup restoration **MUST** be analyzed, and all issues leading to failure **MUST** be fixed. A new backup restoration test **MUST** be performed immediately afterward. This process must be repeated until successful restoration is confirmed.

7.2.1 Scope of Testing

Teams must perform backup restoration tests for each unique backup and recovery plan, rather than for every individual service or database. The goal is to verify the integrity of the backup and recovery process for all services that share the same plan, while avoiding redundant testing. If multiple services follow the same backup and recovery plan (i.e., they have the same storage type, retention policy, backup frequency, and recovery requirements), it is sufficient to conduct restoration tests on one representative service from that group.

Database Selection for Testing:

- Teams **MUST** select databases representative of the plan's complexity and criticality.
- When choosing a database for testing, prioritize more critical or complex databases and select ones from the top.

Testing Environment Requirements:

- Restoration **MUST** be performed in a PROD-like environment (it should be STAGE in most cases).
- There must be no interruption of active production services.
- A backup restoration performed as part of planned infrastructure improvements (e.g., updating the database engine version) can be considered a valid restoration test.

7.2.2 When to Perform

A restoration test **MUST** be performed for High and Medium critical services in the following cases:

● **New Employee Onboarding:**

- Every new team member **MUST** learn how to restore backups for databases under their team's responsibility.
- If the new team member is a Dev On Call, they **MUST** be prepared to restore a database in an emergency.

● **Employee Offboarding (Dismissal/Resignation):**

- To reduce reliance on key individuals (bus factor), we must ensure that knowledge of backup restoration is not limited to a single person.
- The leaving employee **MUST** participate in a final knowledge transfer session covering the restoration process.

● **After Database Engine Updates:**

- Any database engine version upgrade requires a successful backup restoration test to confirm compatibility and integrity.

● **After Major Infrastructure Changes:**

- Changes affecting storage, backup, or networking architecture require validation through restoration testing.
- **After Changes in the Backup and Recovery Plan:**
- Any modification to backup strategy, retention policy, or recovery process **MUST** be followed by a restoration test.
- **At least once every six months.**

7.2.3 Definition of Done

To ensure backups are functional and data integrity is preserved, the following minimal requirements define the **Definition of Done (DoD)** for a backup restoration test:

Data Restoration Validation:

- Validate that the database can be successfully restored from the backup. The restoration process should be completed without errors or warnings.
- Check data integrity (if it is possible)

Service work validation:

- Switch the service to the restored database instance (please note that the testing **MUST NOT** affect PROD services).
- Verify that the service functions correctly and there is no data corruption.

Automation Encouraged:

- Teams are encouraged to automate the restoration and validation process wherever possible to ensure consistency and reduce manual effort.

7.2.4 Documentation and Reporting

All restoration tests must be documented, including:

- Date and time of the test.
- Backup used for restoration.
- Queries or actions performed to validate data integrity.
- Results of the test and any anomalies encountered.

7.3 Monitoring and Responding

7.3.1 Department and Team Level Monitoring

On the department or team level, every failure in the backup process **MUST** be automatically recorded and appropriately marked for further analysis. This ensures continuous monitoring of the backup process, with particular attention to instances of unsuccessful backups. Specialized alert systems **MUST** be configured to notify responsible personnel of any issues that arise promptly.

7.3.2 Questionnaire and Dashboard

To ensure that all storage systems across the company are adequately covered by backup plans, each department is required to provide detailed information about their storages and associated backup strategies. This information is collected via a standardized **questionnaire** and presented in a centralized **Backup Dashboard** for monitoring and auditing purposes.

The questionnaire serves two key purposes:

- To provide visibility into the storage systems and their backup configurations.
- To ensure accountability and compliance with organizational backup policies.

The Backup Dashboard visualizes data from the questionnaire, providing an accessible overview of backup practices, storage criticality, and recovery readiness across the company.

Questionnaire Maintenance and Responsibilities

- **Accountability:** The Head of Engineering (HoE) for each department responsible for specific storage systems **MUST** designate a responsible person(s) for maintaining the questionnaire and addressing any discrepancies or gaps identified through the Backup Dashboard.
- **Initial Submission:** The HoE **MUST** ensure the initial submission of storage and backup information via the questionnaire.
- **Updates:** The questionnaire **MUST** be updated by the designated responsible person(s) whenever there are changes to backup plans, storage configurations, or related systems.
- **Periodic Review:** Even if no changes occur, responsible persons **MUST** review and confirm the accuracy of the information in the questionnaire at least once every six months.
- **Automatic Updates:** For now, only some of the information about AWS-managed databases will be updated automatically in the questionnaire. In future, all teams must make an effort to automate the gathering of information for self-manager or other types of databases.

Dashboard

The **Backup Dashboard** provides a comprehensive view of the collected data, enabling:

- Weekly updates of information from the questionnaire to the Dashboard.
- Identification of storages without active backup plans.
- Monitoring compliance with retention, criticality, and restoration requirements.
- Tracking the status of backup restoration tests and readiness.

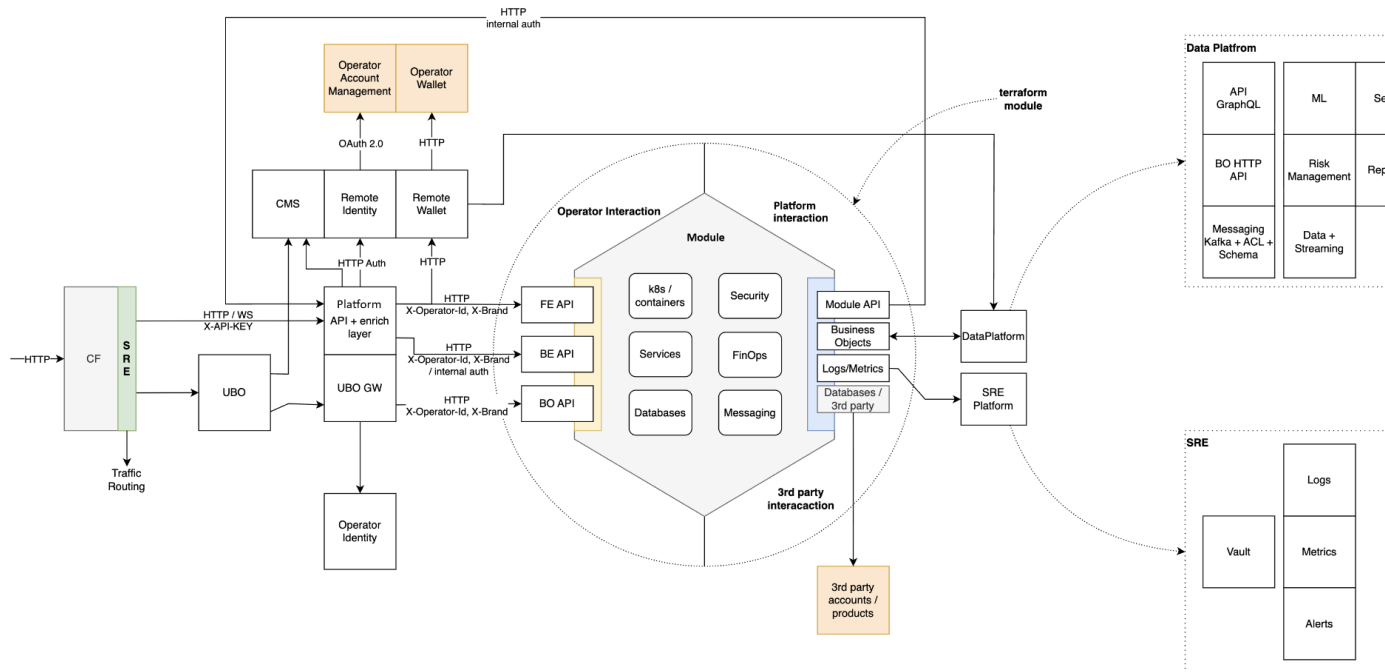
The Dashboard serves as a central tool for both operational oversight and management reporting.

7.4 Review and Compliance

All departments must adhere to the following:

- Ensure that backup plans comply with the criticality and retention requirements outlined in this policy.
- Follow the requirement for restoration tests and perform them in cases described in this policy.
- Respond promptly to any discrepancies or issues identified through the Dashboard or audit processes.
- Keep storage and backup information in the Questionnaire current and accurate.

7.5 Diagram of the technical infrastructure



8. PRINCIPLES OF RESPONSIBLE OPERATION

As required by Article 5.9(1)(g) of the National Ordinance on Games of Chance, this section describes how the principles of responsible gaming have been implemented in the Company's operations, with due regard to the provisions of Article 2.2, third paragraph (responsible offering of Games of Chance), Article 5.4 (prevention of Vulnerable Persons from playing Games of Chance), and Article 5.6 (responsible marketing and advertising). The Company's responsible gaming framework is further aligned with the dedicated Responsible Gaming Policy issued by the CGA, as applicable and as amended from time to time. The following subsections outline the Company's operational measures for ensuring that all gaming activities are offered in a safe, responsible, transparent, and verifiable manner, including the measures taken to prevent participation by Vulnerable Persons and the standards applied to the Company's marketing and advertising activities.

Ownership and Integrity. All Ultimate Beneficial Owners (UBOs), Qualified Interest Holders, and Key Persons are verified and documented. The Company does not cooperate with any individual or entity convicted of crimes such as fraud, money laundering, or terrorism financing.

Financial Compliance. The source of funds and wealth used in operations is verified as legitimate. All license fees, taxes, and contributions are paid and up to date. The Company maintains sufficient liquidity to meet player payout obligations.

Responsible Gaming Framework. The Company enforces a Responsible Gaming Policy to:

- Ensure a safe and fair gaming environment;
- Prevent participation by Vulnerable Persons;
- Provide tools for self-limitation, cooling-off, and self-exclusion to mitigate gambling-related harm.

Regulatory Compliance. The Company participates in approved dispute resolution mechanisms, ensures that no Vulnerable Persons are employed in key roles, and remains registered in the goAML reporting system as required by law.

8.1 Prevention of vulnerable person participation

The Company maintains and enforces a Responsible Gaming Policy aimed at preventing Vulnerable Persons from participating in Games of Chance. This policy includes:

- Awareness and Education – Clear information on gambling addiction and available support resources is accessible to all clients.
- Identification Measures – Verification procedures are in place to identify and restrict Vulnerable Persons.
- Prevention Tools – Systems monitor and mitigate signs of excessive or problematic gambling behavior.

- Self-Exclusion Options – Clients may voluntarily request exclusion from gambling activities for a minimum of twelve (12) months, effective from the date of the request. Such exclusion is irrevocable during the exclusion period.

All procedures comply with applicable ministerial regulations governing responsible gaming and the exclusion of Vulnerable Persons.

8.2. Marketing and advertising standards

The Company ensures that all marketing and promotional activities, including bonuses and incentives, are conducted responsibly and in compliance with applicable regulations. Specifically, the Company guarantees that its marketing and advertising:

- Do not promote excessive or irresponsible gambling;
- Are accurate, transparent, and non-misleading;
- Do not target or appeal to Vulnerable Persons.

All marketing materials are reviewed and approved in line with internal compliance procedures to ensure alignment with responsible gaming principles and regulatory standards regarding content, audience, timing, and placement.

9. TERMS & CONDITIONS

Article 5.9(1)(h) of the National Ordinance on Games of Chance requires the operations manual to contain the most recent text of the general terms and conditions used by the operation. In addition, Article 5.8(k) of the National Ordinance and Article 11 of the Company's License Conditions establish detailed requirements for the content, accessibility, and governance of the Terms and Conditions ("T&Cs"). The CGA has further issued a dedicated Policy Guideline on Terms and Conditions, which sets out comprehensive standards for the scope, structure, and substance of the T&Cs maintained by licensed operators.

The Company's T&Cs are developed and maintained in full compliance with the National Ordinance, the License Conditions, and the CGA Policy Guideline. The T&Cs are clear, unambiguous, transparent, and internally consistent, and are aligned with the Company's internal and external policies, business model, market focus, payment solutions, and promotional practices for each brand or domain to which they apply. Where the Company operates multiple brands, differentiated T&Cs are maintained where necessary, with any differences clearly disclosed.

9.1 Scope of the Terms and Conditions

The Company's T&Cs address the following subject areas, in accordance with the requirements of the National Ordinance, the License Conditions, and the CGA Policy Guideline:

- Disclosure of licensee information, including the Company's legal name, registered business address, Chamber of Commerce registration number, CGA license number, and issue date;
- Governing law (Curaçao) and jurisdiction of the Curaçao courts for all disputes, in accordance with Article 5.5 of the National Ordinance;
- Player eligibility, including minimum age requirements, restricted jurisdictions, and prohibition of third-party registration;
- Player obligations prior to account opening, including the provision of accurate registration details, account security, and prohibition of account transfers;
- Identification and verification (KYC) requirements and procedures;
- AML/CFT obligations, including transaction monitoring and sanctions/PEP screening;
- Data protection and retention, including the collection, use, storage, and sharing of personal data;
- Account closure, suspension, and dormant account procedures, including applicable fees and fund handling;
- Player funds and winnings, including deposit and withdrawal methods, processing timelines, and conditions for fund remittance;
- Non-financial institution status of the Company and the treatment of deposited funds;
- Cancellation or change to wagers, games, and events, including procedures for odds errors, software issues, or live dealer discrepancies;
- Bonuses and promotions, including wagering requirements, expiry periods, and withdrawal conditions;

- Confiscation or limitation of winnings and the applicable conditions;
- Currency rules for bets and prize money, including cryptocurrency-specific provisions;
- Responsible gaming, including deposit limits, self-exclusion, and a reference to the Company's Responsible Gaming Policy;
- Dispute resolution, including the complaints procedure and escalation to ADR, with a reference to the Company's Player Complaints Policy;
- Fairness and game rules, including the use of certified RNGs and the determination of results;
- Liability limitations in cases of technical failure, fraud, or unauthorised access;
- Acceptable player behaviour and consequences of violations;
- Final provisions, including severability, entire agreement, contact details, and periodic review.

9.2 Player Acknowledgment and Amendment Procedures

During registration, players must actively acknowledge acceptance of the T&Cs. Passive acceptance is not sufficient for this purpose. Material changes to the T&Cs require active re-acceptance by the player, including a clear presentation of the nature of the changes, the effective date, and the consequences of rejecting the amended terms. Players are given sufficient opportunity to review changes and determine whether they wish to continue participating. Evidence of player notification is retained and made available to the CGA upon request. Changes to the T&Cs do not apply retrospectively, except where the change does not prejudice the player or the Company is correcting clear technical or contractual errors.

9.3 Accessibility and Availability

The current version of the T&Cs is made available to players at all times in a clear and readable form across all websites, mobile platforms, and other delivery mediums. The T&Cs are accessible within one click from the homepage, registration page, and player account area. Previous versions of the T&Cs are maintained in a historical archive and made available to players upon request.

9.4 Regulatory Submissions and Record-Keeping

The Company maintains a historical archive of all versions of the T&Cs from the date of enactment of the National Ordinance. The current English-language version of the T&Cs is at all times available to the CGA. Where differentiated T&Cs are used for multiple brands, all versions are to be provided. If requested by CGA, the historic versions or non-English versions at its discretion.

9.5 Review and Updates

The T&Cs are reviewed periodically and updated to reflect regulatory developments, CGA guidance, changes to the Company's operations, and evolving industry standards. Any updates are implemented in accordance with the amendment procedures described in this section and in compliance with the CGA Policy Guideline.

10. DISPUTE RESOLUTION FRAMEWORK

This section describes how the Company settles disputes with players, in accordance with Article 5.9(1)(i) and Article 5.3 of the National Ordinance on Games of Chance. The Company maintains a dedicated Player Complaints Policy, which is published on the Company's website, accessible to players at all times, and forms an integral part of the Company's Terms and Conditions.

10.1 Principles

The Company provides all registered players with access to a transparent, fair, and efficient complaint resolution process. Complaints may be submitted free of charge. The Company treats all complaints with impartiality and respect, processes them within clearly defined timelines, and provides reasoned written outcomes. Responsible Gaming complaints are given priority handling due to their potential impact on player well-being. The Company maintains comprehensive records of all complaints and provides reports to the CGA in accordance with applicable reporting obligations.

10.2 Submission and Eligibility

Any registered player may file a formal complaint regarding any Game of Chance within six (6) months of the incident giving rise to the complaint. Third-party complaints are not accepted. Players are encouraged to contact the Company's customer support team in the first instance, as many issues can be resolved through direct assistance without the need for a formal complaint.

Where a matter is not resolved through customer support, the player may submit a formal complaint using the Company's Official Complaint Submission Form, available for download on the Company's website. The form conforms to the requirements of Article 5.3(3) of the National Ordinance and requires the complainant's name, address, and place of residence, the date of the complaint, the language of submission (English, Dutch, or Papiamentu), and a description of the conduct being disputed.

10.3 Handling Procedure

A registered player may file a complaint with the Company, free of charge, within six (6) months after an incident occurred relating to the player's playing of a Game of Chance.

The complaint must be submitted using a template available on a website, which conforms to the guidelines of the CGA. The complaint form must:

- contain the complainant's name, address, and place of residence;
- be dated;
- be written in one of the official languages: English, Dutch, or Papiamentu;
- include a description of the behaviour complained about.

Within one (1) week after receiving the complaint, the Company ensures that a written acknowledgment of receipt is provided to the complainant, accompanied by an explanation of the way the complaint will be handled.

Within four (4) weeks after receiving the complaint, the Company notifies the complainant in writing of:

- where a decision was made not to process the complaint, the reason for not processing the complaint; or
- where a decision was made to process the complaint, the final ruling on the complaint, including supporting particulars, recorded in writing.

The four-week resolution period may be extended once, in writing, by an additional four (4) weeks.

The Company offers its players the opportunity to use alternative dispute resolution at their discretion. The alternative dispute resolution is offered at the expense of the Company.

The Company will comply with all further rules concerning complaints and alternative dispute resolution that may be established by means of a ministerial regulation with general effects under the National Ordinance.

10.4 Escalation to Alternative Dispute Resolution

If a player is not satisfied with the outcome of the internal complaints process, the player has the right to escalate the complaint to an independent Alternative Dispute Resolution (ADR) provider at any time, free of charge, at the Company's expense, in accordance with Article 5.3(6) and (7) of the National Ordinance. The ADR process is impartial and independent from the Company. The ADR provider's decision is binding on both the Company and the player, without prejudice to the player's right to pursue further legal or judicial recourse. Details of the ADR provider, including the provider's name, contact information, and the applicable procedure, are set out in the Company's Terms and Conditions and the Player Complaints Policy.

10.5 Policy Availability

The full Player Complaints Policy, including detailed timelines, submission instructions, and the downloadable Official Complaint Submission Form, is available on the Company's website and is accessible from the player interface at all times. The Policy may be updated from time to time to reflect regulatory developments, CGA guidance, or improvements to the Company's processes. The Company will comply with all further regulatory rules concerning complaints and dispute resolution issued under the National Ordinance.

11. SERVER OF A TIER-IV

Article 5.9(1)(j) of the National Ordinance on Games of Chance requires license holders to maintain digital records of critical information about players, their gaming transactions, and their financial transactions on a server hosted in a Tier-IV certified data center registered in Curaçao, accessible to the CGA at all times.

As of the date of the current version of this Manual, the CGA has not yet finalised the specific technical, operational, or procedural requirements governing the storage of digital records on a Tier-IV certified server in Curaçao. No official list of approved Tier-IV data center providers has been published, and detailed guidance on the scope, format, and access protocols for the required digital records remains pending.

Notwithstanding the above, the Company's existing infrastructure and operational processes are designed to meet or exceed the security, availability, and integrity standards associated with a Tier-IV certified environment, positioning the Company for a seamless transition once the applicable requirements are finalised.

11.1 Current Infrastructure Alignment

The Company's principal data storage and processing infrastructure, as described in Section 5 of this Manual, holds internationally recognised certifications including ISO/IEC 27001, SOC 2 Type II, and PCI DSS Level 1, among others. These certifications reflect compliance with security, availability, and data integrity standards that meet or exceed the control objectives underlying the Tier-IV classification.

11.2 Operational Readiness

The Company's disaster recovery and high availability architecture, as detailed in Section 7 of this Manual, provides multi-site redundancy, automated failover mechanisms, and recovery objectives consistent with the uptime and resilience standards associated with Tier-IV facility design. The Company's security framework, regulatory access capabilities, and data retention practices, as described in Sections 5.4, 5.5, and 5.3 respectively, are structured to operate within a Curaçao-based Tier-IV environment without material modification.

11.3 Preparatory Measures

In anticipation of the finalisation of the CGA's requirements, the Company has undertaken the following preparatory steps:

- **Provider Evaluation.** The Company has identified and evaluated potential Tier-IV certified data center providers in Curaçao, assessing each against criteria including certification status, network connectivity, service-level capabilities, and regulatory alignment.
- **Integration Feasibility.** The Company's technical teams have assessed the feasibility of integrating Curaçao-based server infrastructure into the Company's existing architecture, covering data

synchronisation, latency, failover compatibility, and encryption interoperability.

- **Migration Planning.** The Company has developed a preliminary migration framework outlining the sequencing, testing, and validation steps required to transition to a Curaçao-based Tier-IV facility while maintaining uninterrupted service to players and continuous regulatory access for the CGA.

Once the CGA publishes its finalised requirements, the Company is prepared to implement all necessary changes within the required timeline to maintain full compliance with the National Ordinance on Games of Chance and the conditions attached to its Gaming License. This section of the Manual will be updated upon completion of the migration.

12. STAFF TRAINING AND CONTINUOUS EDUCATION

As required by Article 5.9(4) of the National Ordinance on Games of Chance, this section provides an overview of the Company's education framework applicable to all persons working in the field of Games of Chance within the Company's operations. Training is delivered on a regular basis and is designed to ensure that all relevant personnel maintain a high level of professional competence, regulatory awareness, and ethical standards with regards to their professional duties. The programme is aligned with the broader requirements of the National Ordinance, the conditions attached to the Company's Gaming License, and applicable CGA policies and guidance.

12.1 Training Topics

The Company's annual training programme covers the following core topics, as specified by Article 5.9(4) of the National Ordinance:

- Mental well-being;
- Anti-bribery practices;
- Crime prevention;
- Responsible gaming;
- Anti-money laundering (AML) and countering the financing of terrorism (CFT);
- Effective communication with players;
- Responsible marketing and advertising.

The training programme may be expanded to include additional topics as required by CGA guidance, evolving regulatory standards, or the Company's internal compliance objectives.

12.2 Role-Based Training

All training programmes cover the full scope of mandatory topics listed above, regardless of the employee's position. Each programme is, however, tailored to the employee's specific role, level of responsibility, and prior experience, so that the focus and depth of individual topics reflect the knowledge and competence expected in that role. For example, compliance and risk management personnel receive greater depth on AML/CFT obligations and regulatory reporting, customer-facing employees receive expanded focus on responsible gaming and player communication, and technical staff receive additional emphasis on information security and data protection. This approach ensures that every employee receives comprehensive coverage of all required subjects while also developing the specific expertise relevant to their day-to-day responsibilities.

12.3 Training Frequency

All employees involved in the operation of Games of Chance are required to complete the Company's training programme at least once per calendar year. In addition to the annual cycle, the

Company may conduct ad hoc training sessions during the year where circumstances require, including in response to material changes in applicable laws or regulations, new CGA guidance or policies, significant updates to the Company's internal procedures or operational practices, or findings from internal audits, compliance reviews, or incident investigations. Ad hoc training is mandatory for all affected personnel and is subject to the same monitoring and record-keeping requirements as the annual programme.

12.4 New Employee Onboarding

All newly appointed employees who are involved in the operation of Games of Chance must complete the Company's initial training programme that covers all core topics listed above. No employee may assume operational responsibilities in connection with the Company's gaming activities prior to completion of initial training.

12.5 Monitoring and Record-Keeping

Participation in annual training is compulsory for all relevant personnel. The Compliance Department is responsible for monitoring completion rates, maintaining training records, and following up on any non-completion. Training records include the employee's name, role, training topics completed, date of completion, and the training provider or facilitator. These records are retained in accordance with the Company's data retention policies and are made available to the CGA upon request.

12.6 Review and Continuous Improvement

The Company continuously reviews and updates its training materials to reflect regulatory developments, new CGA guidance, changes in the Company's operations, industry best practices, and lessons learned from internal audits, compliance reviews, and incident reports. The Compliance Department conducts an annual assessment of training effectiveness and adjusts the programme accordingly.

13. PLAYER ACCESS RESTRICTION MEASURES

The Company implements technical and procedural measures to prevent access to Games of Chance by individuals who are not permitted to participate, in accordance with Article 5.9(1)(e) of the National Ordinance on Games of Chance, the conditions attached to the Company's Gaming License, and applicable anti-money laundering and responsible gaming requirements.

The player access restriction measures described in this section operate within the Company's broader compliance framework and draw on the provisions of two dedicated policies provided to the CGA separately and made available to players on the Company's website at all times.

The Company's Responsible Gaming Policy sets out the full framework for player protection, including self-exclusion, deposit and betting limits, cooling-off periods, and vulnerable person identification. The Company's AML/CFT Policy provides additional player protection tools, including sanctions and PEP screening, transaction monitoring, source of funds verification, and risk-based restrictions on player activity. Together, these policies and the measures described in this section form an integrated approach to preventing access by restricted individuals and safeguarding player welfare.

13.1 Registration-Stage Controls

Prior to account activation, the Company performs the following screening and verification procedures:

- **Age Verification.** All prospective players must confirm they are at least eighteen (18) years of age. Account activation is conditional upon successful identity verification, including documentary confirmation of date of birth.
- **Jurisdiction Screening.** The Company verifies each player's country of residence against its list of restricted jurisdictions, as set out in the General Terms and Conditions. Players from restricted jurisdictions are prevented from completing registration.
- **Sanctions and PEP Screening.** As part of the Company's Know-Your-Customer (KYC) procedures, each prospective player is screened against applicable international and local sanctions lists, as well as for Politically Exposed Person (PEP) status. Matches or potential matches trigger enhanced due diligence before account activation may proceed.
- **Internal Restriction Lists.** Prospective players are checked against the Company's internal restriction database, which includes individuals previously excluded, restricted, or flagged for fraud, abuse of platform services, or violations of the Company's Terms and Conditions.

13.2 Ongoing Monitoring and Screening

Following account activation, the Company maintains continuous and periodic screening across the following categories:

- **Sanctions and PEP Monitoring.** All active player accounts are subject to periodic re-screening against updated sanctions and PEP databases in accordance with the Company's AML/CFT policies. Any new match triggers an immediate review by the Compliance Department, which may result in account suspension, enhanced monitoring, or account closure.
- **Internal Fraud and Abuse Monitoring.** The Company operates monitoring systems designed to detect patterns indicative of fraud, collusion, bonus abuse, multi-accounting, or other forms of platform misuse. Flagged accounts are reviewed by the Compliance and Risk Management teams, and may be restricted, suspended, or closed in accordance with internal procedures and the General Terms and Conditions.
- **FATF and FIU Compliance.** The Company restricts access for individuals who are citizens or residents of states identified by the Financial Action Task Force (FATF) as having strategic AML/CFT deficiencies, or states flagged by the Financial Intelligence Unit (FIU) of Curaçao. These restrictions are updated in line with current FATF publications and FIU guidance.

13.3 Responsible Gaming Restrictions

In alignment with the Company's Responsible Gaming Policy and Article 5.4 of the National Ordinance on Games of Chance, the Company enforces the following access restrictions:

- **Self-Exclusion.** Players may voluntarily request exclusion from all gaming activities. Such exclusion is irrevocable during the exclusion period. Self-excluded players are added to the Company's internal exclusion database, and all platform access and marketing communications are suspended for the duration.
- **Deposit and Betting Limits.** Players may set personal deposit limits, betting limits, and cooling-off periods through their account settings. These restrictions are enforced in real time and cannot be relaxed during the active restriction period without observing the applicable waiting period.
- **Company-Initiated Restrictions.** Where the Company identifies indicators of problematic gambling behaviour, it may impose access restrictions, deposit limits, or temporary account suspensions on its own initiative. Affected players are notified and provided with information on available support resources.

- **Vulnerable Person Identification.** The Company maintains procedures to identify and restrict persons who qualify as Vulnerable Persons under the National Ordinance, including persons under eighteen years of age, persons exhibiting problematic gambling behaviour, persons banned from playing by force or at their own request, and persons who have been declared bankrupt or have otherwise lost control or disposal of their property. Where the Company has reasonable grounds to believe that a player is a Vulnerable Person, access to Games of Chance is restricted pending further review.

13.4 Key Person Play Restriction

In accordance with Article 1.3(b) of the National Ordinance on Games of Chance, no person who qualifies as a Key Person of the Company may participate as a player in the Games of Chance offered by the Company. The Company maintains an internal register of all Key Persons and screens this register against the active player database.

13.5 Governance and Review

The Compliance Department bears primary responsibility for the administration and oversight of all player access restriction measures. Restriction lists and screening databases are reviewed and updated on an ongoing basis. The processes described in this section are subject to periodic internal review and are updated to reflect changes in applicable laws, CGA regulatory guidance, international sanctions regimes, FATF publications, and responsible gaming standards.

Castianes B.V. - Operational Manual V1.0

Final Audit Report

2026-06-22

Created:	2026-06-22
By:	Sharella Bitoria (sharella.bitoria@hbmgroup.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAKyrFfy8MeVM9O77q5-nUdE7w-0h9CXDp

"Castianes B.V. - Operational Manual V1.0" History

-  Document created by Sharella Bitoria (sharella.bitoria@hbmgroup.com)
2026-06-22 - 2:53:55 PM GMT
-  Document emailed to Annesol Melaria (annesol.melaria@hbmgroup.com) for signature
2026-06-22 - 2:54:03 PM GMT
-  Document emailed to Herman Oosten (herman.oosten@hbmgroup.com) for signature
2026-06-22 - 2:54:03 PM GMT
-  Email viewed by Herman Oosten (herman.oosten@hbmgroup.com)
2026-06-22 - 3:20:45 PM GMT
-  Document e-signed by Herman Oosten (herman.oosten@hbmgroup.com)
Signature Date: 2026-06-22 - 3:20:59 PM GMT - Time Source: server - Signature Appearance Selected: MOBILE_IMAGE
-  Email viewed by Annesol Melaria (annesol.melaria@hbmgroup.com)
2026-06-22 - 9:17:12 PM GMT
-  Document e-signed by Annesol Melaria (annesol.melaria@hbmgroup.com)
Signature Date: 2026-06-22 - 9:17:31 PM GMT - Time Source: server - Signature Appearance Selected: IMAGE
-  Agreement completed.
2026-06-22 - 9:17:31 PM GMT