

V 1.0

Winlink B.V.

Operational Manual

**OPERATIONAL POLICIES, PROCEDURES & INTERNAL CONTROLS
MANUAL**

Document / Revision History

Document Reference: Winlink B.V. Operational Manual Revision Number: 1.0 Total Pages: Original issue date: Revision date: Effective Date:	Operational Manual
Written by: Kristian Spasov Date:	
Approved by: Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V. Date: 27 July 2026 	

Revision #	Version Date	Description of Changes
1.0		Initial Draft

Contents

OPERATIONS MANUAL

1. DOCUMENT CONTROL

- 1.1 Purpose
- 1.2 Scope
- 1.3 Regulatory Framework
- 1.4 Related Policies
- 1.5 Definitions

2. COMPANY OVERVIEW

- 2.1 Licenced Entity
- 2.2 Business Activities
- 2.3 Organisational Structure
- 2.4 Key Functions and Responsibilities
- 2.5 Outsourced Functions

3. OPERATIONAL MODEL

- 3.1 Customer Journey Overview
- 3.2 Account Registration
- 3.3 Account Verification
- 3.4 Deposits
- 3.5 Gameplay
- 3.6 Bonuses
- 3.7 Withdrawals
- 3.8 Account Closure
- 3.9 Visual Elements and Player Interface

4. GAMING OPERATIONS

- 4.1 Types of Games Offered
- 4.2 Game Providers
- 4.3 Game Configuration
- 4.4 RNG and Fairness Controls
- 4.5 Betting Rules
- 4.6 Settlement of Bets
- 4.7 Jackpot Management
- 4.8 Game Testing and Monitoring

5. PLAYER ACCOUNT MANAGEMENT

- 5.1 Account Creation
- 5.2 Account Verification
- 5.3 Account Restrictions
- 5.4 Dormant Accounts
- 5.5 Duplicate Accounts
- 5.6 Suspended Accounts

6. PAYMENT OPERATIONS

- 6.1 Payment Service Providers
- 6.2 Deposits
- 6.3 Withdrawals

- 6.4 Payment Reconciliation
- 6.5 Failed Transactions
- 6.6 Chargebacks
- 6.7 Protection of Player Funds

7. RESPONSIBLE GAMING

- 7.1 Responsible Gaming Framework
- 7.2 Vulnerable Persons
- 7.3 Self-Exclusion and Cooling-Of
- 7.4 Limits and Controls
- 7.5 Responsible Marketing

Reference:

Responsible Gaming Policy

8. AML/CFT CONTROLS

- 8.1 AML Governance
- 8.2 Customer Due Diligence
- 8.3 Enhanced Due Diligence
- 8.4 Transaction Monitoring
- 8.5 Suspicious Activity Reporting
- 8.6 Sanctions Controls

Reference:

AML/CFT Policy

Business Risk Assessment

Jurisdictional Risk Assessment

9. COMPLAINTS AND DISPUTE RESOLUTION

- 9.1 Complaints Process
- 9.2 Complaint Handling Timelines
- 9.3 Escalation Process
- 9.4 Alternative Dispute Resolution

10. INFORMATION SECURITY

- 10.1 System Architecture
- 10.2 Access Management
- 10.3 Data Protection
- 10.4 Cybersecurity Controls
- 10.5 Backup and Recovery
- 10.6 Incident Management

Reference:

Information Security Policy

11. TECHNICAL INFRASTRUCTURE

- 11.1 Hosting Environment
- 11.2 Production Environment
- 11.3 Disaster Recovery
- 11.4 Business Continuity
- 11.5 Monitoring and Alerting
- 11.6 Change Management
- 11.7 Platform Architecture Diagram

12. RECORD KEEPING

- 12.1 Gaming Records
- 12.2 Customer Records
- 12.3 Financial Records
- 12.4 AML Records
- 12.5 Retention Periods
- 12.6 Server and Data Center Requirements

13. REGULATORY REPORTING

- 13.1 Amendment Reports
- 13.2 Incident Reports
- 13.3 Transaction Reports
- 13.4 Complaints and ADR Reports
- 13.5 Change and Independent Expert Reports
- 13.6 Communication with the Authority

14. TRAINING AND AWARENESS

- 14.1 Annual Training
- 14.2 AML Training
- 14.3 Responsible Gaming Training
- 14.4 Information Security Training
- 14.5 Training Records

1. DOCUMENT CONTROL

1.1 Purpose

The purpose of this Operational Manual is to describe the operational framework, internal controls, procedures, and responsibilities governing the Company's activities in connection with the provision of licenced games of chance.

This Manual establishes the operational standards applicable to all relevant departments, employees, contractors, and service providers involved in the delivery of gaming services and supports compliance with the requirements of the National Ordinance on Games of Chance (LOK), applicable regulations, licence conditions, and internal policies.

The Manual is intended to ensure that gaming operations are conducted in a safe, fair, transparent, secure, and compliant manner while protecting players, maintaining operational integrity, supporting responsible gaming, and preventing the misuse of the Company's products and services.

This document serves as the primary operational reference for the Company's day-to-day activities and should be read in conjunction with all related policies, procedures, standards, and regulatory requirements.

1.2 Scope

This Operational Manual applies to all operational activities performed by or on behalf of the Company in connection with the provision of licenced online gaming services.

The scope of this Manual includes, but is not limited to:

- customer registration and account management;
- player verification and identity controls;
- gaming operations and game management;
- deposit and withdrawal processing;
- responsible gaming measures;
- anti-money laundering and counter-terrorist financing controls;
- sanctions and politically exposed person screening processes;
- customer support activities;
- complaint handling and dispute resolution procedures;
- information security and data protection controls;
- technical infrastructure and system management;
- regulatory reporting and record retention requirements;
- monitoring, oversight, and internal control activities.

This Manual applies to all Team Members.

This Manual shall be read together with all supporting policies, procedures, standards, and guidelines adopted by the Company as part of its governance, compliance, risk management, security, and operational control framework.

1.3 Regulatory Framework

The Company conducts its activities in accordance with the applicable laws, regulations, licence conditions, regulatory guidance, and internal policies governing the provision of online gaming services.

This Operational Manual has been developed with reference to, and shall be interpreted in conjunction with, the following regulatory and governance framework:

External Regulatory Framework

- National Ordinance on Games of Chance (LOK);
- Licence conditions and requirements issued by the Curaçao Gaming Authority (CGA);
- Applicable anti-money laundering and counter-terrorist financing legislation;
- Applicable sanctions legislation and international sanctions obligations;
- Applicable data protection and privacy requirements;
- Applicable consumer protection requirements;
- Any regulatory directives, guidelines, circulars, standards, or notices issued by the Curaçao Gaming Authority from time to time.

Internal Governance Framework

- AML & CFT Policy and Procedures Manual;
- Business Risk Assessment (BRA);
- Jurisdiction Risk Assessment;
- Responsible Gaming Policy;
- Any additional internal procedures, standards, and controls adopted by the Company.

Where a conflict exists between this Manual and applicable laws, regulations, licence conditions, or regulatory directives, the applicable regulatory requirement shall prevail.

This Manual shall be reviewed and updated whenever material regulatory, operational, technological, or business changes occur, and at least in accordance with the Company's regulatory review requirements.

1.4 Related Policies

This Operational Manual shall be read together with all applicable internal policies, procedures, risk assessments, standards, and guidance documents adopted by the Company.

Such documents may include AML, compliance, responsible gaming, risk management, information security, customer protection, operational, and other governance-related documentation where applicable.

1.5 Definitions

For the purposes of this Manual, the following definitions shall apply:

- **2FA** – Two-Factor Authentication.
- **Account Closure (Erasure)** – Complete closure of the Customer's account after the expiration of the term of suspension (blocking) of the Customer's account.
- **ACLs** – Access Control Lists.
- **ADR** – Alternative Dispute Resolution.

- **AML** – Anti-Money Laundering.
- **B2B** – Business-to-Business.
- **B2C** – Business-to-Consumer.
- **BRA** – Business Risk Assessment.
- **Casino** – A website(-s), its back end, system, storage, providing online games of chance under the licence granted to the Company and a group of Team Members maintaining the website.
- **CDD** – Customer Due Diligence.
- **CFT** – Counter-Terrorist Financing.
- **CGA** – Curaçao Gaming Authority.
- **Complaint** – Any written expression of dissatisfaction submitted by a registered player regarding the Company's services, decisions, terms, conduct, or any incident connected to the player's participation in games of chance, where the player expects a response or resolution.
- **CPF** – Counter-Proliferation Financing.
- **Customer** – A registered player holding an account with the Company.
- **Dormant Account** – A customer account where no deposit and/or gaming activity has been recorded for a period exceeding 30 consecutive calendar days.
- **Enhanced Due Diligence (EDD)** – Additional customer due diligence measures applied to higher-risk customers.
- **Game** – Any game of chance offered by the Company under its licence.
- **KYC** – Know Your Customer identification and verification procedures.
- **LOK** – National Ordinance on Games of Chance.
- **Operational Manual (or Manual)** – This document and any approved amendments thereto.
- **PEP** – Politically Exposed Person.
- **Player Account** – A customer account maintained by the Company for participation in gaming activities.
- **PSP** – Payment Service Provider.
- **RBAC** – Role-Based Access Control.
- **Responsible Gaming** – Measures designed to promote safe gambling behaviour and protect vulnerable persons.
- **RNG** – Random Number Generator.
- **Sanctions** – Restrictive measures imposed by national or international authorities.
- **SAR (Suspicious Activity Report)** – An internal or external report relating to potentially suspicious activity.
- **SOF** – Source of Funds.
- **SOW** – Source of Wealth.
- **Team member** – Any physical entity who is an employee, director, officer, contractor, consultant, and outsourced service provider performing activities that may affect the

Company's gaming operations, regulatory obligations, customer protection measures, or compliance framework.

- **The Company** – The licenced gaming operator to which this Manual applies.
- **Third-Party Service Provider** – Any external party providing services supporting the Company's operations.

2. COMPANY OVERVIEW

2.1 Licenced Entity

The Company is Winlink B.V., incorporated under the laws of Curaçao with Company Number 154346, its registered address at Kaya Richard J. Beaujon Z / N, Curaçao and licenced by the Curaçao Gaming Authority to offer games of chance under licence number OGL/2024/886/0978 granted on 09/05/2025 in accordance with the National Ordinance on Games of Chance (Landsverordening op de kansspelen, P.B. 2024, no. 157) licence.

The Company operates under the legal entity specified in its licence application and maintains all required corporate registrations, approvals, and regulatory authorisations necessary for the conduct of its business activities.

The Company provides its licenced activity via further websites:

- winity.com.

2.2 Business Activities

The Company provides online gaming services through its licenced gaming platform(s) in accordance with applicable regulatory requirements and licence conditions.

The Company's principal business activities include:

- provision of online games of chance;
- operation of customer gaming accounts;
- processing of player deposits and withdrawals;
- administration of bonus and promotional programs;
- customer support services;
- implementation of responsible gaming measures;
- performance of anti-money laundering and counter-terrorist financing controls;
- monitoring and protection of gaming integrity;
- management of player complaints and dispute resolution processes.

The gaming products offered by the Company include:

- Online Casino (Slots);
- Live Casino;

The Company operates its gaming services through the licenced brands listed in Section 2.1 of this Manual and any additional domains approved and operated under its gaming licence.

The Company provides its services exclusively on a business-to-consumer (B2C) basis. The Company does not conduct business-to-business (B2B) activities or provide gaming services, platform services, or other gambling-related services to third-party operators.

The Company's activities are directed exclusively at jurisdictions in which the Company is legally permitted to offer online gaming services under applicable laws, regulatory requirements, and the conditions of its Curaçao gaming licence. The Company does not knowingly provide services in prohibited or restricted jurisdictions.

The Company conducts its activities through online channels and utilises approved third-party service providers where necessary to support gaming operations, payment processing, verification, compliance, security, and technical infrastructure.

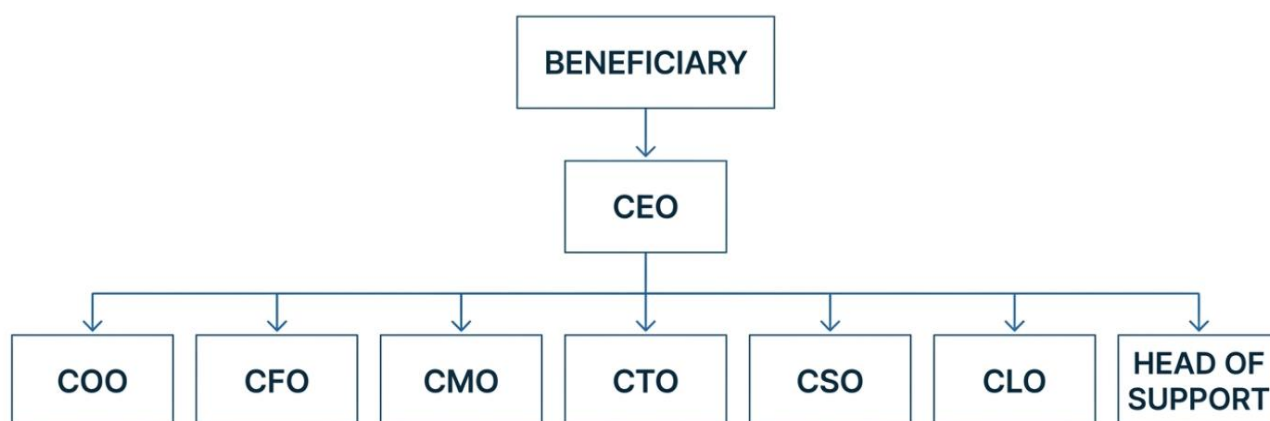
All business activities are performed in accordance with applicable laws, regulatory requirements, internal policies, and operational procedures.

2.3 Organisational Structure

The Company maintains an organisational structure designed to ensure effective governance, operational oversight, regulatory compliance, risk management, and appropriate segregation of duties.

Roles and responsibilities are allocated across management, operational, compliance, technical, financial, and support functions. The organisational structure supports effective decision-making, accountability, and internal oversight.

A high-level overview of the Company's organisational structure is provided below.



2.4 Key Functions and Responsibilities

The Company maintains an appropriate allocation of responsibilities to ensure effective governance, regulatory compliance, operational oversight, risk management, and customer protection.

Chief Executive Officer (CEO)

The Chief Executive Officer (CEO) is responsible for the overall management of the Company's activities, implementation of business strategy, corporate governance, allocation of resources, and oversight of regulatory compliance.

Chief Operating Officer (COO)

The Chief Operating Officer (COO) is responsible for the day-to-day management of the Company's operations, including gaming operations, payment operations, customer support, implementation of operational procedures, and operational performance.

Chief Financial Officer (CFO)

The Chief Financial Officer (CFO) is responsible for financial management, budgeting, financial reporting, treasury management, financial controls, and oversight of financial operations.

Chief Technology Officer (CTO)

The Chief Technology Officer (CTO) is responsible for the Company's technical infrastructure, gaming platform operations, software development, system availability, business continuity, disaster recovery, change management, and technical support.

Chief Security Officer (CSO)

The Chief Security Officer (CSO) is responsible for information security governance, cybersecurity, access management, security monitoring, incident response, protection of information assets, and implementation of information security controls.

Chief Legal Officer (CLO)

The Chief Legal Officer (CLO) is responsible for legal affairs, regulatory legal matters, and overall legal oversight. The CLO manages the Legal Department, which administratively houses key compliance functions, including Anti-Money Laundering (MLRO) and Data Protection (DPO). The CLO ensures these functions receive the necessary legal support, coordination, and resources while strictly respecting their operational independence in statutory decision-making.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) operates within the Legal Department under the administrative oversight of the CLO. The DPO is responsible for overseeing the Company's data protection strategy, ensuring compliance with applicable data privacy laws, and protecting players' personal data. The DPO acts independently in the performance of their statutory privacy duties and maintains a direct reporting line to the Chief Executive Officer (CEO) for the escalation of critical data protection matters.

Money Laundering Reporting Officer (MLRO)

The Money Laundering Reporting Officer (MLRO) operates within the Legal Department under the administrative oversight of the CLO. The MLRO is responsible for the AML/CFT framework and maintains strict operational independence in assessing, investigating, and reporting suspicious activities. The MLRO has direct and unrestricted access to the CEO to ensure that AML/CFT compliance risks are escalated and addressed without undue influence.

Chief Marketing Officer (CMO)

The Chief Marketing Officer (CMO) is responsible for marketing strategy, customer acquisition, promotional activities, brand management, and ensuring that marketing activities comply with applicable legal and regulatory requirements.

Casino Manager The Casino Manager reports to the Chief Operating Officer (COO) and is responsible for the commercial and operational management of the gaming portfolio. This includes the onboarding of game providers, oversight of game configuration, monitoring of RNG certifications, jackpot management, and ensuring that all gaming content complies with applicable regulatory and operational standards.

Head of Support

The Head of Support is responsible for customer support operations, player communications, account-related assistance, complaint handling, escalation of customer concerns, and ensuring that customer interactions are managed in accordance with the Company's policies and regulatory requirements.

All Team Members are responsible for complying with applicable policies, procedures, regulatory requirements, and internal controls relevant to their assigned duties.

2.5 Outsourced Functions

The Company may engage qualified third-party service providers to support certain operational, technical, compliance, security, payment, or administrative activities.

Where outsourced arrangements are implemented, the Company remains fully responsible for compliance with all applicable legal, regulatory, and licence requirements.

Prior to engaging any third-party service provider, the Company shall perform an appropriate assessment of the provider's suitability, competence, reliability, and ability to meet applicable operational and regulatory requirements.

Outsourced service providers shall be subject to contractual arrangements defining the scope of services, responsibilities, service levels, confidentiality obligations, security requirements, and applicable compliance standards.

The Company shall maintain oversight of outsourced functions through ongoing monitoring, periodic reviews, performance assessments, and incident management processes where applicable.

A register of outsourced functions and service providers shall be maintained separately and updated as necessary.

3. OPERATIONAL MODEL

3.1 Customer Journey Overview

The Company has established a structured customer lifecycle designed to provide a secure, transparent, and compliant gaming environment while ensuring an efficient customer experience throughout all stages of the customer relationship.

The customer journey begins with account registration and continues through account verification, deposits, participation in gaming activities, bonus utilisation where applicable, withdrawal processing, and ultimately account closure or termination.

Throughout the customer lifecycle, the Company applies operational controls, fraud prevention measures, responsible gaming safeguards, information security controls, and AML/CFT monitoring processes to ensure compliance with applicable legal, regulatory, and internal requirements.

The customer journey is supported by multiple operational functions, including Customer Support, Payments, Compliance, AML Compliance, Responsible Gaming, Dispute Resolution, Information Technology, and Information Security.

The following sections describe each stage of the customer journey and the controls applied by the Company throughout the customer lifecycle.

3.2 Account Registration

Customers may register an account through the Company's gaming platform in order to access the products and services offered by the Company.

During registration, customers are required to provide accurate and complete information, including personal details, contact information, date of birth, country of residence, and other information requested by the registration process. Registration is available only to individuals who meet the minimum legal age requirements and are legally permitted to participate in online gaming activities.

As part of the registration process, customers must verify their email address and mobile phone number through the verification mechanisms provided by the platform. Account activation may be restricted until the required verification steps have been successfully completed.

The Company operates a one-account-per-customer policy. Customers are prohibited from creating or operating multiple accounts. Controls are implemented to identify and prevent duplicate registrations and account misuse.

The Company applies jurisdictional restrictions and access controls during registration. Registration attempts originating from prohibited, restricted, or otherwise ineligible jurisdictions may be blocked automatically in accordance with legal, regulatory, compliance, and business requirements.

Automated controls are applied during the registration process to support customer verification, fraud prevention, AML/CFT compliance, and platform security. These controls may include screening against restricted jurisdictions, verification of customer contact details, device identification, IP and geolocation checks, risk assessment controls, sanctions screening, PEP screening, and other monitoring activities as determined by the Company's risk management framework.

Customer devices and technical identifiers may be collected and analysed to support fraud prevention, account security, duplicate account detection, regulatory compliance, and risk management activities.

Where registration controls identify potential compliance, fraud, security, responsible gaming, or operational concerns, the account may be subject to additional review, restriction, suspension, or rejection.

Registration-related enquiries and issues are managed through the Company's customer support function. Cases requiring additional investigation or operational review may be escalated to the appropriate second-line support, compliance, AML, fraud prevention, or technical teams.

All registration records are maintained in accordance with applicable legal, regulatory, operational, and record retention requirements.

3.3 Account Verification

The Company applies a risk-based account verification process to confirm customer identity, prevent fraud, ensure platform security, and comply with applicable legal, regulatory, and AML/CFT requirements.

Account verification may be conducted during registration, prior to specific account activities, before the processing of withdrawals, upon reaching predefined transactional thresholds, when risk indicators are identified, or at any other time considered necessary by the Company.

Verification activities may include confirmation of customer contact details, identity verification, address verification, payment method verification, sanctions screening, politically exposed person (PEP) screening, and other customer due diligence measures required under the Company's policies and procedures.

Customers may be required to provide supporting documentation, including but not limited to:

- Government-issued identification documents;
- Proof of residential address;
- Proof of ownership of payment methods;
- Source of Funds (SOF) documentation;
- Source of Wealth (SOW) documentation;
- Any additional information reasonably required to complete verification activities.

The Company performs sanctions and PEP screening as part of its customer due diligence framework. Screening may be conducted during account registration, during account reviews, before withdrawals, and throughout the customer relationship where required by the Company's risk-based approach.

Enhanced Due Diligence (EDD) measures may be applied where elevated risk factors are identified, including high-value transactions, unusual transaction patterns, changes in customer behaviour, high-risk jurisdictions, sanctions or PEP matches, adverse media findings, or other indicators requiring additional review.

Verification activities are performed through a combination of automated internal controls and manual reviews conducted by authorised personnel. Where necessary, verification cases may be escalated to Compliance, AML Compliance, Fraud Prevention, or other authorised functions for further assessment.

Where verification requirements are not satisfied, the Company may impose account restrictions, suspend transactions, reject withdrawal requests, restrict account access, or terminate the customer relationship in accordance with applicable policies and procedures.

All verification records, supporting documents, screening results, and due diligence assessments are maintained in accordance with applicable legal, regulatory, and record retention requirements.

3.4 Deposits

The Company allows customers to fund their gaming accounts using approved payment methods made available through the gaming platform.

All deposit transactions are processed in accordance with applicable legal, regulatory, operational, security, and AML/CFT requirements. Customers may only use payment methods that belong to them and are authorised for use on the platform.

The Company does not accept cash deposits. Deposits may only be made through approved electronic payment channels and payment service providers authorised by the Company.

Prior to accepting deposits, the Company may apply various controls including customer verification, jurisdictional restrictions, sanctions screening, fraud prevention measures, payment verification controls, and other risk management procedures.

The Company reserves the right to restrict, reject, delay, or review deposit transactions where regulatory, compliance, fraud, security, responsible gaming, or operational concerns are identified.

Deposit activity forms part of the Company's ongoing customer monitoring framework. Deposit patterns, transaction behaviour, and other relevant indicators may be reviewed for fraud prevention, responsible gaming, and AML/CFT purposes.

Customers may be required to provide additional information or documentation in support of deposit activity where required by applicable policies, risk assessments, or regulatory obligations.

All deposit transactions are recorded and maintained within the Company's systems and are subject to applicable record retention requirements.

Details of approved payment methods and payment service providers are maintained separately and may be updated from time to time in accordance with operational and business requirements.

3.5 Gameplay

Following successful account registration, verification where applicable, and account funding, customers may participate in the gaming products offered through the Company's platform.

The Company provides access to approved gaming products in accordance with applicable legal, regulatory, licensing, and operational requirements. Customers are responsible for ensuring that their participation in gaming activities complies with the laws applicable in their jurisdiction.

All gaming activity is recorded within the Company's systems and is subject to monitoring, security controls, and operational oversight.

The Company maintains measures designed to ensure the integrity, fairness, and security of gaming activities. Gaming products made available through the platform are subject to applicable testing, certification, and regulatory requirements where required.

During gameplay, the Company may apply operational controls, responsible gaming measures, fraud prevention controls, information security safeguards, and AML/CFT monitoring processes as part of its ongoing customer oversight framework.

The Company reserves the right to restrict, suspend, cancel, or otherwise intervene in gaming activity where regulatory, compliance, fraud, security, responsible gaming, technical, or operational concerns are identified.

Records relating to gaming activity are maintained within the Company's systems in accordance with applicable legal, regulatory, operational, and record retention requirements.

3.6 Bonuses

The Company may offer bonuses, promotions, loyalty rewards, and other incentive programmes to eligible customers in accordance with applicable business, regulatory, and operational requirements.

The availability, eligibility criteria, terms, conditions, and restrictions applicable to bonuses and promotions are communicated separately through the Company's platform and supporting documentation.

Bonus awards may be subject to predefined conditions, including verification requirements, promotional rules, wagering requirements, responsible gaming controls, fraud prevention measures, and compliance reviews where applicable.

The Company maintains controls designed to ensure that bonuses and promotions are awarded, managed, and redeemed in a fair, transparent, and controlled manner.

The Company reserves the right to refuse, restrict, suspend, adjust, cancel, or reclaim bonuses and promotional benefits where abuse, fraud, multiple account activity, regulatory concerns, technical errors, responsible gaming concerns, or violations of applicable terms and conditions are identified.

Bonus activity may be monitored as part of the Company's fraud prevention, responsible gaming, operational monitoring, and AML/CFT control framework.

All bonus-related transactions, adjustments, and promotional activities are recorded within the Company's systems and retained in accordance with applicable legal, regulatory, and operational requirements.

3.7 Withdrawals

Customers may request withdrawals of available funds from their gaming accounts using approved withdrawal methods supported by the Company.

All withdrawal requests are subject to applicable operational, security, fraud prevention, responsible gaming, and AML/CFT controls prior to processing.

Before a withdrawal is approved, the Company may perform account verification, customer due diligence, payment method verification, sanctions screening, PEP screening, transaction reviews, and other control measures deemed necessary under the Company's policies and procedures.

The Company may require customers to provide additional information or supporting documentation before a withdrawal request can be processed.

Withdrawal requests may be delayed, restricted, suspended, or rejected where verification requirements remain outstanding or where regulatory, compliance, fraud, security, responsible gaming, or operational concerns have been identified.

The Company applies controls designed to ensure that withdrawals are made only to the verified customer and through approved payment channels in accordance with applicable legal, regulatory, and operational requirements.

Customer activity may be reviewed as part of the withdrawal process to identify unusual, suspicious, fraudulent, or otherwise prohibited activity requiring further assessment.

Where necessary, withdrawal cases may be escalated to Compliance, AML Compliance, Fraud Prevention, Payments, or other authorised functions for review and decision-making.

All withdrawal requests, reviews, approvals, rejections, and supporting records are maintained within the Company's systems in accordance with applicable legal, regulatory, and record retention requirements.

3.8 Account Closure

Customer accounts may be closed either at the customer's request or by the Company in accordance with applicable legal, regulatory, compliance, responsible gaming, security, fraud prevention, and operational requirements.

Customers may request account closure through the available communication channels or by using account management tools provided through the platform, where available.

The Company may restrict, suspend, deactivate, or permanently close an account where required by law, regulatory obligations, internal policies, responsible gaming measures, AML/CFT requirements, fraud prevention controls, security concerns, or violations of applicable terms and conditions.

Prior to account closure, the Company may perform appropriate reviews to determine whether outstanding verification requirements, active investigations, unresolved disputes, pending transactions, responsible gaming restrictions, regulatory obligations, or other operational matters remain outstanding.

Any eligible customer funds remaining on the account shall be handled in accordance with applicable legal, regulatory, and operational requirements.

Following account closure, customer records, transaction history, due diligence records, communications, and other relevant information shall be retained in accordance with applicable record retention requirements.

Account closure does not affect the Company's obligation to maintain records, fulfil regulatory reporting obligations, cooperate with competent authorities, or continue any ongoing compliance, fraud prevention, security, or AML/CFT investigations where required.

All account closure actions, reviews, decisions, and supporting records shall be maintained within the Company's systems in accordance with applicable legal, regulatory, and operational requirements.

3.9 Visual Elements and Player Interface

The Company ensures that all visual elements presented to players through its websites, mobile applications, or software interfaces comply with regulatory requirements and promote a transparent, safe gaming environment.

- **Brand and Licensing:** The Operator's branding and logo are clearly visible. The footer of the website and application contains the Curaçao Gaming Authority (CGA) digital seal, licensing details, and a clear visual indicator that gambling by minors is prohibited (18+ icon).

- **Responsible Gaming and Support:** Links to the Responsible Gaming Section, self-assessment tools, and problem gambling support resources are prominently displayed in the footer and are easily accessible from the account screens.
- **Navigation and Information:** Links to the General Terms and Conditions, Privacy Policy, and Complaints procedures are permanently accessible, ensuring they are no more than one click away from the homepage.
- **Gaming Interface:** Game rules, odds, risks, and betting limits are clearly accessible to the player before and during gameplay. Banners, bonus displays, pop-ups, and promotional messages are designed to be clear, transparent, and do not target vulnerable players.

Visual elements are maintained consistently across both desktop and mobile versions of the platform. Any material changes to the player-facing interface are subject to internal compliance review and approval.

4. GAMING OPERATIONS

4.1 Types of Games Offered

The Company offers a range of online games of chance through its licenced gaming platform(s) in accordance with applicable legal, regulatory, and licence requirements.

The gaming products offered by the Company include:

- Online Casino (Slots);
- Live Casino;

The availability of specific gaming products, game titles, and game providers may differ between the Company's brands, websites, and licenced domains. Such differences may arise as a result of the integration status of individual game providers, commercial decisions, technical availability, jurisdictional restrictions, or licence-specific requirements applicable to a particular brand or website.

The Company ensures that only games approved for the relevant brand, jurisdiction, and applicable licensing framework are made available to customers. Access to gaming products is controlled through platform configuration, jurisdictional restrictions, and operational controls to ensure compliance with applicable legal, regulatory, and licensing requirements.

The rules of play, betting parameters, outcome-determining mechanisms, and other game-specific characteristics are determined by the respective game providers and are made available to players through the gaming platform before participation in the relevant game.

4.2 Game Providers

The Company utilizes approved third-party game providers to supply gaming content through its licenced gaming platform(s).

All game providers are subject to the Company's onboarding and due diligence procedures and must meet applicable legal, regulatory, licensing, security, and operational requirements before their games are made available to customers.

The integration of game providers is performed in accordance with the Company's technical and operational procedures. The availability of individual providers and their games may vary between the Company's brands, websites, and jurisdictions depending on commercial decisions, integration status, technical availability, and applicable licensing or regulatory requirements.

The Company periodically reviews its integrated game providers to ensure continued compliance with applicable legal, regulatory, and operational requirements.

4.3 Game Configuration

The Company maintains procedures governing the onboarding, configuration, publication, modification, and removal of gaming content available through its licenced gaming platform(s).

The onboarding of a new game provider is initiated following approval by the Chief Operating Officer (COO). Once approved, implementation activities are coordinated through the Company's internal operational procedures. These activities include technical integration, preparation of the gaming database, testing, and marketing readiness. Prior to production release, promotional materials, game assets, and supporting content are obtained from the provider and prepared for deployment. Where a provider offers a large number of games, the rollout may be performed in stages to support operational stability and marketing activities.

New games are added to the platform in accordance with the release schedules communicated by individual game providers. The Operations Team monitors upcoming releases, prepares the required platform configuration, adds the games to the internal database, performs functional testing, and verifies that the games operate correctly and do not create unintended bonus or promotional abuse scenarios before publication. Following successful verification, newly released games are published on the platform and presented to customers through the Company's promotional channels where applicable.

The review and launch of new providers and games involve the Casino Manager, Operations Team and, where required, the relevant Account Manager. The Casino Manager is responsible for approving the publication, temporary suspension, or permanent removal of games from the platform. Such decisions may be based on commercial considerations, provider availability, technical issues, operational requirements, regulatory obligations, or compliance considerations.

Following launch, the gaming catalogue is continuously managed by the Casino Manager and the Operations Team. This includes monitoring game availability, introducing newly released titles, retiring obsolete content, updating game categorisation, and maintaining the overall quality and presentation of the gaming portfolio.

Changes to game configurations, game availability, and operational settings are implemented through the Company's internal operational procedures. Where applicable, configuration changes are reviewed by the responsible operational personnel and verified before being applied to the production environment to ensure that they do not adversely affect game functionality, customer experience, or regulatory compliance.

Changes to gaming content are managed in accordance with the Company's internal operational and change management practices. Depending on the nature of the change, this may include coordination between the Casino Manager, Operations Team, technical personnel, and the relevant game provider to ensure that updates are implemented in a controlled manner and that any identified issues are resolved before or after deployment.

The Company maintains audit logs of changes made within the administrative platform. Change records include the responsible user, the affected configuration or game setting, the previous and updated values, and the date and time of the change. These records support operational oversight, troubleshooting, internal audit, and regulatory compliance.

4.4 RNG and Fairness Controls

The Company offers games supplied by approved third-party game providers. Where Random Number Generator (RNG) technology is required, the RNG mechanisms are provided and maintained by the respective game providers. The Company does not operate proprietary RNG systems for determining game outcomes.

The Company requires that games made available through the platform comply with applicable legal, regulatory, and licensing requirements, including requirements relating to fairness, integrity, and randomness. Game providers are responsible for ensuring that their games, RNG systems, and

associated software are independently tested and certified before being made available for commercial use.

The Company relies on certifications and testing performed by independent testing laboratories accepted within the online gaming industry to demonstrate the fairness and integrity of RNG-based games. Supporting certification documentation is maintained by the respective game providers and made available where required for regulatory or compliance purposes.

Responsibility for monitoring the validity of game certifications and ensuring that providers continue to meet applicable licensing and regulatory requirements rests with the Casino Manager. During the onboarding of new providers and as part of the ongoing relationship with existing providers, the Company verifies that the provider continues to satisfy the applicable operational and regulatory requirements.

Customer complaints relating to game fairness, game outcomes, or technical irregularities are initially handled by Customer Support and escalated to the second-line support team for investigation. Where necessary, the matter is further escalated to the relevant game provider and may involve the Casino Manager, Operations Team, Quality Assurance, or technical personnel until the issue has been investigated and resolved.

The Company may temporarily suspend or permanently remove a game from the platform where there are reasonable grounds to believe that the game no longer complies with applicable legal, regulatory, licensing, technical, or operational requirements, or where technical defects, certification issues, provider actions, or integrity concerns could affect the fairness or proper operation of the game.

Relevant correspondence, investigation records, and supporting documentation relating to game fairness reviews are retained in accordance with the Company's record retention procedures.

4.5 Betting Rules

The Company establishes and maintains a comprehensive framework of player-facing rules governing participation in all gaming activities offered through its licenced brands. These rules are published on the respective brand websites and form part of the contractual relationship between the Company and its customers. By registering an account and using the Company's services, customers acknowledge and accept the applicable rules, policies, and conditions governing the use of the gaming platform.

Player participation is regulated through the following documents, as applicable to each brand:

- Terms and Conditions;
- Registration, Deposits, Withdrawals and Bonus Rules;
- Responsible Gaming Policy;
- Self-Exclusion Policy;
- AML & KYC Policy;
- Privacy Policy;
- Fairness Policy;
- Dispute Resolution Policy.

These documents collectively regulate customer eligibility, account registration, identity verification, deposits, withdrawals, betting activity, bonus participation, account security, responsible gaming obligations, dispute resolution, suspension and closure of accounts, prohibited activities, and other conditions governing the Company's gaming services.

General betting rules applicable across all gaming products require players to use a verified personal account, comply with the published Terms and Conditions, participate only where legally permitted, and refrain from fraudulent, abusive, or prohibited conduct. The Company reserves the right to refuse, suspend, void, or restrict participation where required by applicable legislation, regulatory requirements, internal policies, or where breaches of the applicable rules are identified.

Bonus funds, free spins, promotional credits, cashback offers, and other incentives are governed by the Registration, Deposits, Withdrawals and Bonus Rules together with the specific terms applicable to each promotion. These rules establish eligibility criteria, activation conditions, wagering requirements, validity periods, withdrawal conditions, maximum winnings where applicable, restrictions on bonus abuse, and the circumstances under which promotional benefits or related winnings may be cancelled, forfeited, or recovered.

The Company reviews and updates its player-facing rules whenever required by changes to applicable legislation, regulatory requirements, licensing conditions, operational processes, gaming products, or commercial offerings. Updated versions are published on the relevant brand website before or on the date they become effective. Players are informed of such changes through publication on the website and, where appropriate, by notifications delivered through the player account, website interface, or other communication channels. Continued use of the Company's services following the effective date of the updated rules constitutes acceptance of the revised terms in accordance with the applicable Terms and Conditions.

Responsibility for the preparation, maintenance, and periodic review of the Company's player-facing rules is shared between the Compliance, Legal, Product and Casino Operations, with operational input provided where required. Amendments are reviewed through the Company's internal governance process prior to publication to ensure continued compliance with applicable legal, regulatory, and licensing requirements.

4.6 Settlement of Bets

The Company processes the settlement of gaming transactions through automated integrations with authorised third-party game providers. When a customer places a wager, the betting request is transmitted to the relevant game provider via secure system integration. The game provider determines the game outcome and returns the settlement result, which is processed automatically by the Company's gaming platform.

Upon placement of a wager, the corresponding stake is deducted from the customer's gaming balance. Following receipt of the settlement response from the game provider, any winnings or other resulting balance adjustments are automatically applied to the customer's gaming account. All settlement activities are processed electronically without manual intervention under normal operating conditions.

Manual settlement or balance adjustments are performed only in exceptional circumstances, such as technical failures, interrupted transactions, provider communication issues, or other operational incidents affecting the normal settlement process. Before any manual adjustment is made, the transaction is reviewed to verify the correctness of the settlement and determine the appropriate corrective action.

Disputed gaming transactions and settlement-related customer enquiries are investigated by the appropriate operational functions, which may include Customer Support, Risk, Second-Line Support (L2), Account Management, the Casino Manager, and Operations personnel, depending on the nature of the issue. Where necessary, the Company requests the relevant game provider to verify the transaction and confirm the settlement result before any corrective action is taken.

The investigation process may include verification of the recorded game history, reconciliation of the customer's account balance before and after the transaction, review of transaction records, and examination of communication logs exchanged with the relevant game provider. Where the Company's records confirm that the settlement was processed correctly, the matter may be referred

to the game provider for further investigation. Where an error is confirmed, the Company performs the appropriate balance correction. Where necessary to protect the integrity of the investigation or comply with operational or regulatory requirements, customer account restrictions, including temporary withdrawal restrictions or account suspension, may be applied until the matter has been resolved.

The Company maintains comprehensive records of gaming transactions and settlement activities. These records include the game history, transaction history, and balance history reflecting each account movement, including wagers, winnings, rollbacks, returned bets, and any authorised balance adjustments. Such records support operational monitoring, dispute resolution, audit, and regulatory compliance.

The authoritative game result is determined by the relevant game provider and communicated to the Company's platform through the established system integration. The Company records the received settlement result within the gaming transaction history and customer balance records. Where manual intervention is required following a technical incident, settlement verification and any balance adjustments are performed in accordance with the Company's incident management and operational procedures.

4.7 Jackpot Management

The Company offers jackpot-enabled games provided by authorised third-party game providers. Depending on the game and provider, jackpot functionality may include progressive jackpots and other jackpot mechanisms operated in accordance with the provider's game rules. The technical operation, jackpot calculations, winner selection, and prize determination are performed by the relevant game provider.

Commercial oversight of jackpot-enabled games is performed by the Casino Manager, while the technical operation and administration of jackpot functionality remain the responsibility of the respective game provider.

For progressive jackpots, the jackpot prize pool is established in accordance with the provider's jackpot configuration. Depending on the provider's requirements, a starting jackpot amount may be contributed before the jackpot becomes available, or the jackpot may commence at a predefined minimum value. Thereafter, a specified proportion of eligible wagers is automatically contributed to the jackpot prize pool. Fixed jackpots, where applicable, form part of the game's predefined payout structure and are funded in accordance with the game provider's game design.

Jackpot winners are determined automatically and randomly by the relevant game provider in accordance with the applicable game rules and jackpot mechanics. The Company does not independently determine jackpot winners.

Following confirmation of the jackpot result by the game provider, jackpot winnings are automatically credited to the customer's gaming balance and recorded as part of the corresponding gaming transaction. Settlement is performed without manual intervention under normal operating conditions.

Specific jackpot eligibility criteria, participation requirements, and promotional conditions are established by the relevant game provider. Depending on the provider's rules, participation may be limited to designated games, minimum wager amounts, or other qualifying conditions. Certain wager types, including free spin rounds where applicable, may be excluded from jackpot participation.

Jackpot winnings are normally processed automatically. Where a technical failure, disputed settlement, or other operational exception affects a jackpot transaction, the Company verifies the settlement with the relevant game provider before any balance adjustment is performed. For significant jackpot wins, additional verification may be conducted where necessary to confirm the accuracy of the settlement.

The Company maintains records of jackpot-related gaming transactions through its game history, gaming transaction records, and customer balance history. In addition, the Company maintains

monthly records of aggregate jackpot contribution amounts and jackpot winnings relating to network jackpots. For certain local jackpots, operational monitoring of the current jackpot value may also be performed to support business and promotional activities. These records support operational monitoring, customer dispute resolution, audit, and regulatory compliance.

4.8 Game Testing and Monitoring

The Company continuously monitors gaming products following their deployment to ensure their availability, integrity, and correct operation. Ongoing monitoring includes daily analysis of game performance and operational statistics, review of customer support enquiries, risk monitoring activities, and automated quality assurance testing designed to identify operational or technical issues affecting gaming services.

Responsibility for monitoring the operational performance of gaming products is shared between the Quality Assurance (QA) function, the Casino Manager, and Operations personnel responsible for gaming content. These functions monitor game availability, operational performance, and customer-reported issues and coordinate corrective actions where necessary.

Gaming incidents include, but are not limited to, game malfunctions, customer complaints relating to game operation, incorrect settlement of wagers or winnings, and errors affecting the recording of gaming rounds or other gaming transactions.

Potential technical issues are identified through operational monitoring, analysis of game statistics, review of expected operational results, automated testing, and customer reports. Where abnormal behaviour or operational issues are identified, the Company investigates whether the issue originates within its own systems or the relevant game provider's systems. Where necessary, the affected game may be temporarily withdrawn from service while the investigation is conducted. If the issue is determined to originate with the game provider, the Company raises the matter with the provider for investigation and resolution.

Communication with game providers regarding technical or operational issues is coordinated by Second-Line Support (L2), Account Management, and the Casino Manager, as appropriate.

Where a game is temporarily removed from service, it is placed into maintenance mode and identified on the gaming platform as temporarily unavailable until normal operation has been restored.

Gaming incidents are documented through the Company's incident tracking system. Incident records include reported issues, investigation activities, communications with the relevant game provider where applicable, corrective actions, and resolution status.

The Company prioritises remediation activities according to the severity and business impact of the identified issue. Responsible team leads monitor the progress of corrective actions to ensure that issues are resolved within appropriate timeframes and that service is restored as soon as reasonably practicable.

5. PLAYER ACCOUNT MANAGEMENT

5.1 Account Creation

Following successful registration, a player account is created within the platform together with the associated internal records. As part of the account creation process, customer registration data is stored, a customer profile is established, an AML Risk Profile is created, and an initial risk assessment is performed.

During onboarding, automated checks are conducted, including sanctions screening, PEP screening, and the calculation of the customer's initial risk rating. The results of these checks are

used to determine the customer's risk classification and any applicable monitoring or verification requirements.

5.2 Account Verification

Following account creation, the customer is assigned an appropriate verification status. The verification status determines the availability of certain account functions and may change depending on the completion of KYC, CDD, or EDD procedures.

Account verification is performed in accordance with the Company's AML/CFT framework and risk-based approach. Depending on the customer's risk profile, activity, and transactional behaviour, the Company may apply simplified, standard, or enhanced verification measures.

Where required by internal procedures or applicable regulatory requirements, customers may be requested to provide additional documentation or refresh previously submitted documents. Certain account functions may be restricted until the required verification has been successfully completed.

5.3 Account Restrictions

Customer accounts may be subject to restrictions for the purposes of AML/CFT compliance, Responsible Gaming, Fraud Prevention, operational security, or other regulatory and business requirements.

Restrictions may affect specific account functions, including account access, deposits, withdrawals, and access to gaming products.

Authorised members of the Customer Support and Risk departments may apply account restrictions in accordance with internal procedures. Restrictions may also be applied following reviews, investigations, or assessments conducted by other relevant functions within the Company.

Restrictions may be initiated by AML, Fraud Prevention, Responsible Gaming, Risk Management, Operations, or other authorised functions, depending on the nature of the identified risk or circumstance.

Each restriction is recorded within the administrative system through the appropriate account status. Supporting records are maintained within the customer profile, including details of the reason for the restriction, the date applied, the responsible function, and any related internal investigation or case reference.

Account restrictions may be removed once the underlying circumstances have been resolved and all required reviews have been completed. Where restrictions were applied following the assessment or request of a specific department, their removal shall be subject to confirmation from the relevant responsible function.

5.4 Dormant Accounts

A customer account is considered dormant where no deposit and/or gaming activity has been recorded for a period exceeding 30 consecutive calendar days.

Dormant accounts remain active within the Company's systems unless suspended, closed, or restricted for other regulatory or operational reasons. Customers retain access to their accounts subject to the applicable Terms and Conditions and any regulatory requirements.

Dormant customers may be included in customer reactivation campaigns conducted by the Company. Such campaigns may include promotional offers or other marketing communications designed to encourage customers to resume gaming activity. All marketing communications are carried out in accordance with applicable legal, regulatory, responsible gaming, and customer marketing preferences.

5.5 Duplicate Accounts

The Company enforces a strict one-account-per-customer policy. The creation of duplicate accounts is strictly prohibited. The Company utilizes automated systems and authorized personnel to monitor registrations and identify potential duplicate accounts. In exceptional circumstances, such as the loss of access credentials, a customer may be permitted to open a new account only with explicit prior approval from the relevant operational department. If a duplicate account is identified without prior authorization, the Company reserves the right to block or close any or all associated accounts. The Risk Management and Fraud Prevention teams are responsible for assessing such cases and may render void any bets placed via duplicate accounts. Furthermore, if fraudulent intent is determined, the Company may withhold the refund of initial deposits and/or bonuses.

5.6 Suspended and Closed Accounts

Customer accounts may be suspended (blocked) or closed either upon the customer's request or at the Company's discretion in accordance with internal policies and the applicable Terms and Conditions. Account closure constitutes the complete deactivation of the account following the expiration of any suspension period.

Account suspension may also be triggered by a customer exercising their right to self-exclusion for a defined period. During a suspension period, the Company retains the customer's personal data in accordance with defined retention schedules (e.g., 5 years from the date of the last financial transaction, or 1 month if no financial transactions were recorded).

Following account closure, eligible funds are handled according to internal procedures; however, bonus funds or free spins are not subject to refund or encashment unless authorized by management. Customers are granted a 14-day calendar period to appeal a Company-initiated blocking or closure decision.

Authorized personnel may immediately block a customer's account without prior notice under specific conditions, including but not limited to situations where:

- the Company decides to cease providing services to a specific customer based on internal risk assessments;
- the account is linked to another previously closed or blocked gaming profile;
- there is suspicion of system hacking or participation in collusion;
- the customer interferes or attempts to manipulate the software;
- the customer uses their account for illegal purposes;
- the customer publishes defamatory or offensive information about the Company;
- there is a material violation of the Terms and Conditions;
- the Company receives a valid request from the customer to erase their personal data.

6. PAYMENT OPERATIONS

6.1 Payment Service Providers

The Company utilizes approved Payment Service Providers ("PSPs") to facilitate deposits and withdrawals in accordance with applicable legal, regulatory, operational, AML/CFT/CPF, fraud prevention, and information security requirements. Payment Service Providers are selected using a risk-based approach to ensure the reliability, security, and continuity of payment services provided to players.

The Company maintains internal records of all approved Payment Service Providers together with the relevant contractual, operational, technical, and compliance documentation. Such records form part of the Company's operational documentation and are maintained separately from this Manual.

Roles and Responsibilities

The Finance Department, together with the Business Development team, is responsible for identifying, evaluating, and selecting potential Payment Service Providers based on commercial, operational, and regulatory considerations. The Technical Department is responsible for the technical integration, configuration, testing, and deployment of approved PSPs into the Company's gaming platform.

Following implementation, the Payment Operations Team is responsible for the ongoing operational supervision of all payment providers. This includes continuous monitoring of service availability, transaction processing, incident management, communication with PSPs, and coordination of corrective actions where required.

Pre-Onboarding Due Diligence

Before a new Payment Service Provider is approved for integration, the Company performs a risk-based due diligence assessment appropriate to the nature, jurisdiction, and risk profile of the provider. The assessment may include:

- verification of the legal existence, ownership structure, licensing status, and regulatory authorisations of the PSP;
- assessment of financial stability, operational capacity, and business continuity arrangements;
- collection of market feedback and review of the provider's reputation within the payment industry;
- screening of publicly available adverse media and other relevant public information;
- verification against applicable international sanctions lists and, where appropriate, politically exposed person (PEP) information relating to beneficial owners or senior management;
- assessment of the provider's AML/CFT, fraud prevention, and compliance framework;
- review of information security controls, data protection measures, and, where available, recognised security certifications or independent audit reports;
- evaluation of supported payment methods, settlement capabilities, processing performance, geographical coverage, and technical compatibility with the Company's platform;
- review of contractual terms, including service level commitments, incident notification procedures, security obligations, and regulatory cooperation requirements.

Where a prospective PSP has limited operational history or insufficient market reputation, the Company may apply additional risk mitigation measures, including enhanced due diligence, limited production rollout, increased transaction monitoring, transaction limits, security deposits, or other appropriate safeguards before full implementation.

Ongoing Monitoring

The operational performance of each Payment Service Provider is monitored on a continuous basis. The Payment Operations Team performs daily reviews of key operational indicators, including transaction success rates, processing times, settlement performance, system availability, failed transactions, error rates, and recurring operational issues.

Any service degradation, operational disruption, security event, or other material incident is promptly investigated in cooperation with the relevant Payment Service Provider. Incidents are recorded in accordance with the Company's incident management procedures, and corrective actions are tracked until resolution. Where recurring deficiencies, unacceptable performance, or compliance

concerns are identified, the Company may require remediation measures, implement enhanced monitoring, suspend the affected payment method, or discontinue cooperation with the PSP following an internal risk assessment.

6.2 Deposits

Customers may fund their gaming accounts only through the payment methods made available within the gaming platform. The availability of payment methods may vary depending on the customer's jurisdiction, applicable regulatory requirements, supported currencies, technical availability, and the Company's internal risk controls.

To initiate a deposit, the customer selects one of the available payment methods and submits a deposit request through the gaming platform. Deposited funds are credited to the customer's gaming account only after successful payment authorisation and confirmation of the transaction.

The Company applies a risk-based approach to deposit processing. Depending on the customer's risk profile, transaction characteristics, jurisdiction, or other relevant risk indicators, additional verification measures may be applied before, during, or after the processing of a deposit. Where required to comply with applicable legal, regulatory, AML/CFT/CPF, fraud prevention, or payment security requirements, the Company may verify ownership or lawful control of the payment instrument used for the transaction and request additional information or supporting documentation from the customer.

The Company may delay, suspend, decline, or reverse a deposit where required to comply with applicable legal, regulatory, AML/CFT/CPF, fraud prevention, responsible gaming, payment provider, or internal risk management requirements.

All deposit transactions are recorded within the Company's systems and include, where applicable, the transaction identifier, payment method, currency, transaction amount, transaction status, timestamps, and other information necessary for operational processing, financial reconciliation, customer support, compliance monitoring, regulatory reporting, and audit purposes.

Deposit transactions are subject to ongoing automated and manual monitoring as part of the Company's AML/CFT/CPF, fraud prevention, and operational risk management framework. Transaction behaviour, payment patterns, geographic indicators, customer activity, and other relevant risk indicators may result in additional reviews, customer due diligence, enhanced verification measures, or other appropriate actions in accordance with the Company's internal policies and applicable regulatory requirements.

6.3 Withdrawals

Customers may request withdrawals of available funds from their gaming account using approved withdrawal methods supported by the platform.

Prior to processing a withdrawal request, the Company may perform verification, security, AML/CFT, fraud prevention, responsible gaming, and other risk-based reviews as required by applicable regulations and internal procedures. Additional customer information or documentation may be requested where necessary.

Withdrawal requests are reviewed in accordance with the Company's pay-out management procedures. The Company may delay, reject, reverse, or place a withdrawal request under review where additional verification, compliance review, or investigation is required.

Once approved, funds are transferred to the customer through the relevant payment method and the transaction is recorded within the Company's systems. Withdrawal transactions form part of the Company's ongoing monitoring framework and may trigger customer risk reassessments, AML reviews, or additional due diligence measures where applicable.

The Company maintains complete records of withdrawal requests, approvals, rejections, payment processing outcomes, and any related compliance or operational reviews.

6.4 Payment Reconciliation

The Company performs payment reconciliation to verify the completeness, accuracy, and consistency of all payment transactions processed through the gaming platform and Payment Service Providers. The reconciliation process covers customer deposits, withdrawals, internal payment transfers, settlement transactions, and other payment-related operations.

Reconciliation is performed on both an individual transaction basis and an aggregate basis by comparing transaction records maintained within the Company's gaming platform, payment processing microservices, and internal financial systems against transaction records, settlement reports, and operational reports available through the back-office systems of the respective Payment Service Providers or official reports provided directly by the PSP.

Payment reconciliation is performed on a daily basis and additionally as part of the monthly financial closing process to ensure the accuracy and completeness of the Company's financial records.

The Finance Department is responsible for performing payment reconciliation. Operational assistance is provided by the Payment Operations Team, which is responsible for monitoring the operational performance of payment providers, investigating payment processing issues, coordinating communication with PSPs, and supporting the resolution of payment-related incidents.

Where discrepancies are identified, reconciliation is performed by comparing transaction records maintained within the gaming platform, payment processing microservices responsible for deposit and withdrawal processing, and the corresponding records maintained by the relevant Payment Service Provider. Any identified mismatch is analysed to determine its origin and impact. Where a discrepancy cannot be resolved internally, the matter is escalated through the Payment Operations Team to the designated financial or operational representatives of the relevant PSP for investigation and resolution. All material discrepancies and corrective actions are documented and tracked until fully resolved.

The reconciliation process produces and maintains reconciliation records, settlement reports, accounting records maintained within the Company's financial systems (including QuickBooks and 1C), together with supporting documentation required for financial reporting, operational oversight, regulatory compliance, and audit purposes.

6.5 Failed Transactions

The Company maintains procedures for the identification, classification, monitoring, investigation, and resolution of failed payment transactions in order to ensure the reliability and integrity of payment processing.

All payment processing errors, declined transactions, and failure responses received from Payment Service Providers are automatically captured by the Company's payment processing systems. Error responses are mapped and classified according to predefined error categories to enable consistent processing, operational monitoring, statistical analysis, incident management, and reporting.

Failed deposit transactions are subject to daily operational analysis to identify anomalies, recurring failures, unusual transaction patterns, and potential degradation of payment processing performance. The Company maintains an automated alerting system designed to detect abnormal payment behaviour and notify the appropriate operational personnel for further investigation.

Failed withdrawal transactions are subject to the same daily operational analysis and automated alerting processes. In addition, the status of all withdrawal transactions is continuously monitored by the Payment Operations Team, which oversees payout processing operations and ensures that

delayed, failed, rejected, or otherwise abnormal withdrawal transactions are promptly identified, investigated, and, where appropriate, escalated for resolution.

The Payment Operations Team is primarily responsible for investigating failed payment transactions and coordinating their resolution. Depending on the nature of the incident, the Business Development Team and Technical Department may participate in the investigation to determine the root cause, implement corrective measures, and coordinate with the relevant Payment Service Provider where necessary.

Customers are informed of unsuccessful payment transactions directly through the cashier interface of the gaming platform. Where a payment transaction cannot be completed, an appropriate on-screen message is displayed informing the customer that the transaction has failed or could not be processed successfully. Where additional assistance is required, the customer may contact Customer Support for further guidance.

Information relating to failed payment transactions, identified anomalies, recurring issues, investigation results, and corrective actions is retained as part of the Company's operational records. Trend analysis and operational metrics derived from failed transactions are used to improve payment processing performance, optimise alerting mechanisms, strengthen operational controls, and support the Company's risk management, fraud prevention, and AML/CFT/CPF frameworks.

6.6 Chargebacks

The Company maintains procedures for the identification, assessment, recording, and management of chargeback notifications received from Payment Service Providers or payment schemes.

The Business Department and Risk Management function are responsible for reviewing chargeback cases, assessing the associated risks, and determining the appropriate course of action in accordance with the Company's internal procedures and contractual arrangements with the relevant Payment Service Provider.

Upon receipt of a chargeback notification, the affected customer account is immediately restricted from further payment activity while the case is reviewed. Additional account restrictions may be applied where required in accordance with the Company's fraud prevention, AML/CFT/CPF, and risk management procedures.

Customer account restrictions remain in place throughout the chargeback review process. Depending on the outcome of the investigation and the assessed level of risk, the Company may maintain, modify, or remove the applied restrictions in accordance with its internal policies.

The Company maintains operational communication with the relevant Payment Service Providers regarding chargeback notifications, settlement information, and case status updates. Where appropriate, chargebacks may be reviewed to determine whether supporting information should be provided to the PSP. Where a decision is made not to dispute a chargeback, the transaction is processed in accordance with the applicable rules, contractual arrangements, and procedures established by the relevant Payment Service Provider.

All chargeback cases are recorded within the Company's operational records. Chargeback-related metrics, including the annual chargeback rate and fraud rate, are calculated and reviewed at least once each calendar year as part of the Company's operational risk management and fraud monitoring processes.

6.7 Protection of Player Funds

The Company maintains operational and financial controls designed to safeguard customer funds, minimise counterparty risk, and ensure the continuity of payment operations.

To reduce operational and counterparty concentration risks, the Company distributes payment processing activities across multiple approved Payment Service Providers. This diversification

strategy reduces dependence on any single provider and supports the uninterrupted processing of customer deposits and withdrawals.

Where the Company engages Payment Service Providers with limited operating history, reduced market presence, or where payment methods present an elevated operational risk, additional financial safeguards may be implemented. Such safeguards may include the use of secured collateral arrangements, security deposits, or other contractual mechanisms designed to mitigate potential financial exposure.

The Company also performs regular settlements and daily transfers of funds from Payment Service Provider balances to Company-controlled accounts in order to minimise the amount of customer funds held by third parties and reduce operational and counterparty risks.

Responsibility for the protection and oversight of customer funds is shared across several departments. The Treasury Department is responsible for monitoring the security, availability, and allocation of customer funds. The Risk Management Department oversees compliance, AML/CFT/CPF, fraud prevention, and financial risk management activities affecting customer funds. The Financial Control and Analysis Department performs reconciliations, verifies account balances, and confirms the accuracy and completeness of financial records.

Where an operational or financial incident affects customer funds, the Company applies a risk-based incident management process appropriate to the nature and severity of the event. Material incidents are escalated without undue delay to senior management and, where necessary, to senior representatives of the relevant Payment Service Provider to facilitate prompt investigation and resolution.

Where appropriate and considered necessary to protect customers and maintain confidence in the Company's services, the Company may reimburse affected customers before the incident has been fully resolved with the relevant Payment Service Provider. Any such decision is made on a case-by-case basis following an assessment of the operational, financial, regulatory, and customer impact of the incident.

All material incidents affecting customer funds are documented, investigated, and reviewed to identify root causes, implement corrective actions, and strengthen the Company's operational controls and risk management framework.

7. RESPONSIBLE GAMING

7.1 Responsible Gaming Framework

The Company is committed to promoting Responsible Gaming principles and maintaining a safe and controlled gaming environment for all players. Gambling is intended solely as a form of entertainment and should not be regarded as a source of income. Players are provided with information regarding the risks associated with excessive gambling and are offered tools to help control and manage their gaming activities. The Company supports measures aimed at preventing gambling addiction and provides access to self-restriction and self-exclusion mechanisms.

The Company regularly informs players about the signs of problem gambling and recommends seeking assistance from specialized support organizations, including Gamblers Anonymous, Gambling Therapy, and GamCare.

Furthermore, the Company ensures that players are informed about responsible gaming risks through a clearly identifiable and easily accessible Responsible Gaming Section on the website and/or application. A clear and visible link to this section is displayed on the homepage and in the footer. The footer also includes a clear visual indication that gambling by minors is prohibited (18+), the Operator's licence details, the CGA digital seal, and links to gambling addiction support resources.

7.2 Vulnerable Persons

Individuals under the age of 18, or under the legal age for gambling in their respective jurisdiction, are prohibited from accessing the Company's services. The Company takes reasonable measures to prevent underage persons from accessing its gaming services. During registration, players must confirm they are over 18, and government-issued valid identification is verified before the first withdrawal.

The Company considers players displaying indicators of problem gambling to be potentially vulnerable persons. Such indicators may include:

- continuously increasing betting amounts;
- attempts to recover gambling losses through further gambling activity;
- use of borrowed funds for gambling purposes;
- adverse impact of gambling on personal, family, or professional life;
- inability to control gambling behaviour;
- use of gambling as a means of escaping personal difficulties or emotional distress.

To proactively detect risky behaviour, the Company operates behaviour tracking controls using system-based alerts, player account data, and transactional monitoring (e.g., sudden increases in deposit frequency, repeated failed transactions, or inexplicably extended play sessions).

All responsible gaming interactions, whether initiated by the player or the Company, are documented in the Player Account Management (PAM) system and retained for at least five years. Where vulnerability is identified, the Company intervenes by applying mandatory deposit limits, temporarily suspending the account, or excluding the player where the risk is severe.

7.3 Self-Exclusion and Cooling-Off

The Company provides players with the ability to voluntarily self-exclude or temporarily restrict access to gaming services through the Responsible Gaming Section.

Cooling-Off Periods: Players may activate a cooling-off period for any of the following durations:

- 24 hours;
- 7 days;
- 1 month;
- 3 months. During a cooling-off period, the player is restricted from gambling activity, while funds remain available for withdrawal.

Self-Exclusion: Players may also activate a Self-Exclusion period for the following durations:

- 1 year;
- 3 years;
- 5 years;
- 10 years;
- Lifetime. During self-exclusion, the player's account is closed, login is blocked, deposits and wagering are prohibited, and direct marketing is stopped. Self-exclusion applies to all brands or domains operated under the Company's licence. Following the expiry of a self-exclusion period, accounts are not automatically reactivated and require positive confirmation from the player.

7.4 Limits and Controls

The Company makes responsible gaming tools available to players, allowing them to manage their gambling behaviour. The following limits and controls are implemented:

- **Deposit Limits:** Customers may set deposit limits for daily, weekly, or monthly periods. Once a limit is reached, further deposits are blocked. Any request to make a deposit limit more restrictive takes effect immediately, while any request to make a limit less restrictive is subject to a 24-hour waiting period before implementation.
- **Loss Limits:** A limit on a Customer's losses for 24 hours, a week, or a month. The loss calculation is based on the initial deposit and does not include winnings attributed to the deposited amount. For instance, if a customer deposits €50 and sets a Loss Limit of €10, and subsequently wins €1,000, the customer may still lose more than €10 of the €1,000 balance, as the limit applies strictly to the initial deposit rather than the accumulated winnings.
- **Additional Controls:** Depending on the jurisdictional and operational risk profile, the Company may also offer loss limits, wager limits, time/session limits, and player-activated reality checks (pop-up reminders) to ensure players remain aware of their activity.
- **Self-Assessment:** Players have access to their betting and wagering history, as well as self-assessment resources to evaluate their gambling habits.

7.5 Responsible Marketing

The Company ensures that all marketing and advertising communications strictly comply with responsible gaming standards. The following procedures are enforced:

- **Protection of Vulnerable Groups:** Marketing and advertising are never knowingly or deliberately directed at minors, vulnerable persons, or players showing indicators of problematic gambling.
- **Self-Excluded Players:** The Company ensures that all direct marketing, promotional emails, and bonuses are strictly suspended for players who have activated a cooling-off period or self-exclusion.
- **Misleading Content Prevention:** Advertising must not portray gambling as an investment, a route to financial success, a solution to financial or emotional difficulties, or a substitute for well-being. It must not misrepresent the role of chance or suggest that skill can influence purely chance-based games.
- **Risk Warnings:** All advertising material includes a clearly visible responsible gaming message or slogan.
- **Third-Party Compliance:** Affiliates, influencers, and other third parties involved in marketing are explicitly informed of the Company's Responsible Gaming Policy and are contractually required to comply with it. Marketing consent is collected transparently during registration or via account settings.

8. AML/CFT CONTROLS

8.1 AML Governance

The Company maintains an AML/CFT framework designed to identify, assess, monitor, and mitigate risks associated with money laundering, terrorist financing, and proliferation financing.

Overall oversight of the AML/CFT programme is exercised by the Company's executive management, which is responsible for ensuring adequate resources, effective governance arrangements, and implementation of a risk-based approach throughout the organisation.

For AML/CFT purposes, the Company appoints a Money Laundering Reporting Officer (MLRO) and maintains appropriate arrangements to ensure continuity of AML/CFT functions, including investigations, reporting obligations, and liaison with competent authorities.

AML/CFT controls are supported through the coordinated efforts of the AML/Compliance, Risk Management, Finance, Customer Support, and other operational departments within their respective areas of responsibility.

The AML/CFT Policy and related AML/CFT procedures are reviewed at least annually or whenever significant changes occur in the Company's business activities, applicable legislation, or regulatory requirements.

Employees receive AML/CFT training appropriate to their roles and responsibilities, and the effectiveness of the AML/CFT framework is subject to periodic independent assessment.

8.2 Customer Due Diligence

The Company applies a risk-based approach to customer identification and verification in accordance with its AML/CFT framework and internal procedures.

Customer Due Diligence measures are performed when establishing a business relationship, prior to certain financial transactions, upon reaching established AML thresholds, and whenever the customer's activity, risk profile, or available information requires additional review.

Customer verification is conducted using the Company's internal procedures and systems without the use of external identity verification providers.

As part of the Customer Due Diligence process, the Company collects and verifies information necessary to identify the customer and assess the associated level of risk, including identity document details, residential address information, payment method information, contact details, and any additional information required to establish and verify the customer's identity.

The Company also assesses the purpose and intended nature of the business relationship and establishes an initial customer risk profile based on customer, jurisdictional, product, and transactional risk factors.

Customer information is maintained and updated throughout the business relationship. Where necessary, the Company may request updated documentation, additional information, or conduct re-verification procedures.

Where the Company is unable to satisfactorily complete Customer Due Diligence measures, verify the customer's identity, or obtain sufficient information to assess customer risk, the Company may refuse to establish or continue the business relationship, restrict account activity, or apply other measures in accordance with its AML/CFT procedures.

Documents, information, and verification results obtained through the Customer Due Diligence process are retained in accordance with the Company's record keeping and AML/CFT requirements.

8.3 Enhanced Due Diligence

The Company applies Enhanced Due Diligence (EDD) measures to customers, transactions, and business relationships that present an elevated level of risk under the Company's risk-based approach.

EDD may be applied upon reaching established financial thresholds as well as where circumstances require additional review or enhanced scrutiny.

Circumstances that may result in the application of Enhanced Due Diligence include:

- attempts to structure transactions or circumvent established thresholds;

- execution of a series of related transactions;
- significant changes in a customer's financial behaviour;
- significant changes in a customer's gaming activity;
- use of payment methods or transaction patterns inconsistent with the customer's profile;
- activity that is inconsistent with previously obtained customer information;
- indicators of unusual or potentially suspicious activity;
- an increase in the customer's risk level;
- any other circumstances which, in the Company's opinion, require enhanced review for AML/CFT purposes.

As part of the Enhanced Due Diligence process, the Company may request additional information and documentation necessary to understand the customer's activities, source of funds, and overall risk profile.

Source of Funds (SoF) information may be requested where it is necessary to verify the origin of funds used by the customer, including cases involving significant financial activity, large deposits or withdrawals, substantial changes in customer behaviour, elevated risk levels, or other circumstances requiring additional review.

Source of Wealth (SoW) information may be requested where it is necessary to establish the origin of a customer's overall wealth, including higher-risk customers, customers with substantial transaction volumes, or other situations where the Company's AML/CFT risk assessment requires additional verification.

As part of EDD, the Company may apply additional control measures, including enhanced monitoring of customer activity, additional verification procedures, collection of supplementary documentation, management involvement in the review process, and other measures appropriate to the level of identified risk.

Where the Company is unable to obtain sufficient information to complete the Enhanced Due Diligence process, or where the level of risk is considered unacceptable, the Company may refuse to establish or continue the business relationship, restrict account activity, or terminate the customer relationship in accordance with its internal procedures.

8.4 Transaction Monitoring

The Company conducts ongoing monitoring of customer activity throughout the duration of the business relationship as part of its risk-based AML/CFT framework.

The purpose of Transaction Monitoring is to identify unusual activity, activity inconsistent with the customer's profile, potentially suspicious behaviour, or other activity that may indicate money laundering, terrorist financing, fraud, or other financial crime risks.

Monitoring is performed through a combination of automated controls and manual reviews conducted by authorised AML/Compliance personnel.

As part of its monitoring activities, the Company reviews:

- deposits and withdrawals;
- transaction volumes and frequency;
- payment methods used;
- customer gaming activity;

- customer behaviour and changes in activity patterns;
- customer risk profiles;
- changes to customer registration data and account information;
- other AML/CFT risk factors identified through the Company's internal procedures.

Transaction Monitoring is used to identify activity requiring additional review, investigation, reassessment of customer risk, application of Enhanced Due Diligence measures, or escalation to the MLRO.

Where unusual or potentially suspicious activity is identified, the Company may request additional information or documentation, conduct further customer reviews, apply enhanced monitoring measures, temporarily restrict certain account functions, or initiate an internal investigation in accordance with its AML/CFT procedures.

Monitoring results, reviews, investigations, decisions, and actions taken are documented and retained in accordance with the Company's internal record keeping requirements.

8.5 Suspicious Activity Reporting

The Company maintains procedures for the identification, investigation, escalation, and reporting of unusual or potentially suspicious activity as part of its AML/CFT framework.

Any employee who identifies unusual activity, activity inconsistent with a customer's profile, or potentially suspicious behaviour is required to promptly escalate the matter to the AML/Compliance function for further review.

Reported matters are recorded within the Company's case management system and assigned for assessment by the MLRO.

As part of the review process, the MLRO considers all relevant information available to the Company, including customer information, Customer Due Diligence and Enhanced Due Diligence records, transaction history, monitoring results, internal notes, previous reviews, and any other information relevant to the case.

Where necessary, the Company may request additional information or documentation, perform additional reviews, apply enhanced monitoring measures, or take other actions required to complete the investigation.

Following completion of the review, the MLRO determines whether sufficient grounds exist to classify the activity as suspicious and whether a report should be submitted to the relevant competent authority.

The preparation and submission of suspicious activity reports are performed by the MLRO in accordance with applicable legal and regulatory requirements.

Reports are submitted without undue delay following completion of the internal review and determination that external reporting is required.

All investigations, decisions, supporting materials, and actions taken in relation to suspicious activity reviews are documented and retained within the Company's case management system in accordance with applicable record keeping requirements.

The Company maintains measures designed to prevent tipping-off. Information relating to ongoing investigations, case reviews, reporting decisions, or the submission of reports is not disclosed to customers or unauthorised persons.

Customer communications relating to AML/CFT reviews are limited to requests for information and documentation necessary to complete the Company's verification, monitoring, and investigation procedures.

8.6 Sanctions Controls

The Company operates sanctions controls as an integral part of its AML/CFT framework and applies a risk-based approach to identifying individuals subject to international sanctions or classified as Politically Exposed Persons (PEPs).

Sanctions and PEP screening is conducted during customer onboarding and as part of ongoing due diligence and enhanced verification activities.

The sanctions screening process incorporates:

- international sanctions lists;
- Politically Exposed Persons (PEP) databases;
- specialised compliance monitoring tools;
- official government sources;
- publicly available media sources;
- social media and other open-source intelligence resources.

Ongoing sanctions screening is performed as part of periodic customer reviews, risk profile updates, enhanced due diligence procedures, and whenever circumstances require reassessment of sanctions-related risks.

Where a potential sanctions match is identified, additional verification is performed using supplementary customer information and supporting documentation to determine whether the match is genuine.

Temporary restrictions may be applied to the account while the review is ongoing.

Where a sanctions match is confirmed, the account will be closed and any further actions will be taken in accordance with the Company's internal procedures and applicable legal and regulatory requirements.

Sanctions-related reviews are conducted by the AML/Compliance function and the MLRO.

Where a potential sanctions match is identified by Customer Support, Risk Management, Finance, or any other department, the matter must be immediately escalated to the MLRO for investigation and final determination.

9. COMPLAINTS AND DISPUTE RESOLUTION

9.1 Complaints Process

The Company is committed to handling customer complaints in a fair, transparent, and timely manner. A complaint is defined as any written expression of dissatisfaction submitted by a registered player regarding the Company's services, decisions, terms, conduct, or any incident connected to the player's participation in games of chance, where the player expects a response or resolution.

The Customer may submit complaints free of charge within six months from the settlement of the bet or the incident giving rise to the complaint. Complaints may first be directed to customer support via email and/or live chat. Furthermore, the Company makes an official Complaint Submission Form available to players. This form is accessible as a downloadable document and/or as an online form that can be completed and submitted directly through the website or player account.

When submitting a complaint, players are required to provide, at a minimum: the Customer's name, address, place of residence, account number (where applicable), the date of the complaint, the date

of the disputed event, and a description of the disputed conduct or transaction. The Company may request supporting documents reasonably required to investigate the matter.

Complaints are initially handled by Customer Support. Depending on the subject matter, complaints are escalated to the relevant internal department (e.g., Payments, Gaming Operations, KYC/Verification, AML/Compliance, Legal, or Management). Responsible gaming complaints are strictly prioritized and handled with the appropriate involvement of trained Responsible Gaming or Compliance personnel.

9.2 Complaint Handling Timelines

The Company enforces strict timelines for the acknowledgement and resolution of customer complaints depending on their nature:

- **Responsible Gaming Complaints:** These are treated as priority matters. The Company confirms receipt in writing within two (2) business days, explaining how the complaint will be processed and providing an expected timeline. The Company uses its best efforts to resolve these complaints within five (5) business days. If more time is required for an informed decision, the player is notified of the delay, which may not exceed two (2) weeks. If the delay is caused by the player (e.g., lack of requested information), the period may be extended by a maximum of an additional two (2) weeks.
- **Standard Complaints:** For all other complaints, the Company confirms receipt in writing within one (1) week, detailing the processing steps and average timeline. The Company assesses and responds to these complaints within four (4) weeks. If complexity or lack of information requires more time, this period may be extended once by an additional four (4) weeks, provided the player is informed in writing before the original deadline expires.

In all cases, the Customer receives a final determination in writing, which includes a reasoned final assessment of the complaint and the outcome, supported by evidence where necessary.

9.3 Escalation Process

Where a complaint cannot be resolved at the initial review stage, it may be escalated to a higher level of management, such as Customer Support Management, Risk/Compliance personnel, the MLRO (for AML/CFT matters), or Senior Management.

The Company documents all complaints, decisions, and escalations in a dedicated Complaint Register. Each record includes player details, complaint category, summary of the issue, requested/received documents, departments involved, investigation steps, the final outcome (e.g., upheld, rejected, settled, referred to ADR), and response dates. The escalation process includes a thorough review of this register, previous communications, and supporting evidence. The decision reached following internal escalation represents the Company's final internal determination of the matter.

9.4 Alternative Dispute Resolution

If a player remains dissatisfied with the final outcome of the internal complaints process, they are informed of their right to escalate the complaint to an independent, CGA-approved Alternative Dispute Resolution (ADR) provider free of charge.

The Company will fully cooperate with competent regulatory authorities, authorized ADR bodies, and other legally competent institutions where required by applicable law. Records of unresolved complaints and complaints escalated to ADR or legal proceedings are retained for the required period and made available to the Curaçao Gaming Authority (CGA) upon request.

10. INFORMATION SECURITY

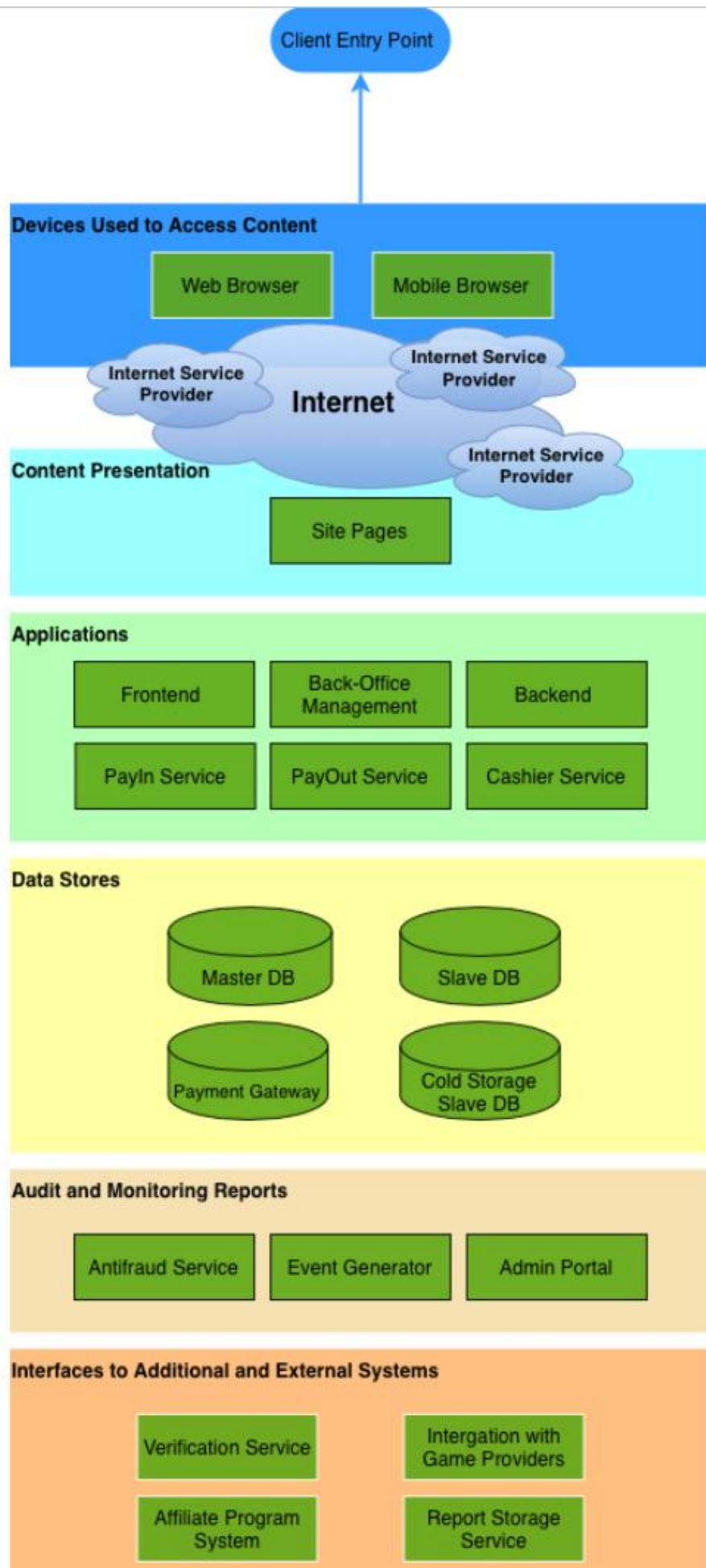
10.1 System Architecture

The Company's platform architecture consists of the core systems, supporting services, and external integrations required for the operation of the gaming platform.

The principal components of the platform include:

- Website pages used for content presentation and management;
- Back-Office Management application;
- Administrative Portal;
- Identity Verification Service;
- Report Storage Service;
- Affiliate Program System;
- Integration with licenced Game Providers;
- PayIn Service, including Cashier Service;
- PayOut Service;
- Master Database, Slave Database, and Cold Storage Slave Database.

A high-level overview of the Company's platform architecture is provided in the System Architecture Diagram below.



The Company utilizes a hybrid software architecture comprising both proprietary systems developed in-house and integrated third-party solutions. While core platform functionalities may be maintained internally, specialized operational modules—including game aggregation, payment processing gateways, identity verification (KYC), and AML monitoring systems—are supplied by approved third-party B2B providers. The exact composition of proprietary versus third-party software may evolve based on operational and commercial needs. All third-party systems and external software modifications are subject to the Company's strict onboarding, security assessment, and change management procedures prior to deployment.

10.2 Access Management

The Company maintains documented access management procedures governing the granting, modification, periodic review, and revocation of access to systems, applications, and infrastructure.

All requests relating to the granting, modification, or revocation of user access rights and administrative privileges are submitted and processed exclusively through the Company's corporate task tracking system. Each request records the requestor, the person performing the change, the business justification, and the date and time of the action, ensuring a complete audit trail of access-related changes.

Administrative privileges ("admin" access) are assigned only to authorised technical personnel responsible for administering the Company's systems and infrastructure. The principal roles assigned administrative access include:

- Security Officers;
- NOC Engineers; and
- DevOps Engineers.

Access rights are reviewed in accordance with the Company's internal procedures applicable to each system and, in all cases, no less frequently than once every three (3) months.

Where supported by the relevant system, Two-Factor Authentication (2FA) is implemented as an additional authentication mechanism.

10.3 Data Protection

The Company implements technical and organisational measures to protect personal data, corporate information, and operational data from unauthorised access, disclosure, alteration, or loss.

Key data protection measures include:

- encryption of data in transit using TLS/HTTPS;
- encryption of data at rest using AES-256 for Amazon Aurora databases and backups;
- Role-Based Access Control (RBAC);
- Access Control Lists (ACLs);
- IP allowlists;
- regular audit log reviews; and
- the use of Virtual Private Networks (VPNs) where applicable.

Personal data and operational data are stored on isolated database servers supported by regular backup procedures.

Access to data is restricted through Role-Based Access Control (RBAC), Access Control Lists (ACLs), and IP allowlists in accordance with the applicable system configuration.

Data is retained in accordance with the Company's data retention requirements and is automatically deleted upon expiry of the applicable retention period or following a valid data subject request, where applicable.

10.4 Cybersecurity Controls

The Company maintains a cybersecurity control framework designed to protect its information assets, gaming platform, and supporting infrastructure against unauthorised access, cyber threats, data compromise, and service disruption. Cybersecurity controls are implemented through a combination of preventive, detective, and corrective measures proportionate to the Company's operational and regulatory requirements. Responsibility for the oversight of the cybersecurity framework rests with the Chief Security Officer (CSO).

The Company's cybersecurity controls include identity and access management, Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), Access Control Lists (ACLs), IP allowlists, network security controls, web application protection, encryption where appropriate, continuous monitoring, centralised logging, administrative activity auditing, and secure backup arrangements. These controls are designed to preserve the confidentiality, integrity, and availability of the Company's systems and information assets.

The Company applies a risk-based approach to vulnerability management. Security vulnerabilities identified through monitoring activities, security assessments, or external vulnerability scanning are evaluated, prioritised, and remediated according to their potential impact and business risk. Security patches and software updates are implemented through the Company's change management process following appropriate review and testing. Regular external vulnerability scanning is performed to support the identification of security weaknesses and the verification of implemented security controls.

Security testing is performed where appropriate to verify the effectiveness of cybersecurity controls and to identify potential weaknesses within the Company's technical environment. Testing activities may include vulnerability assessments, security scanning, verification of implemented security controls, and security testing associated with significant infrastructure or application changes. Identified findings are assessed and remediated in accordance with the Company's risk management and change management procedures.

The Company maintains continuous monitoring and security alerting capabilities to support the timely detection, investigation, escalation, and response to security events. Security-relevant events and administrative activities are logged and monitored to facilitate incident investigation, operational oversight, and regulatory compliance. Cybersecurity incidents are managed in accordance with the Company's Incident Management procedures under the coordination of the Chief Security Officer and the responsible technical personnel.

10.5 Backup and Recovery

The Company maintains backup arrangements to preserve the availability, integrity, and recoverability of critical systems and information assets in the event of system failure, data corruption, cybersecurity incidents, or other operational disruptions.

Scheduled backups are performed for critical production systems, databases, application data, system configurations, and other information required to maintain the continuity of the Company's licenced gaming operations. Backup activities are monitored to verify their successful completion.

Backup data includes, where applicable, gaming platform databases, customer account information, transaction records, operational system data, application configurations, security-related information, audit logs, and other business-critical information. Backup copies are protected against unauthorised access and retained in accordance with the Company's data retention, operational, and regulatory requirements.

Backup arrangements form part of the Company's business continuity and disaster recovery framework and support the timely restoration of critical systems and data following a disruption.

The Company periodically tests restoration procedures to verify the integrity, availability, and recoverability of backed-up data. Test results are documented, and any identified issues are addressed through the Company's corrective action and continuous improvement processes.

10.6 Incident Management

The Company maintains an incident management framework to ensure that operational, technical, information security, and compliance-related incidents are identified, recorded, classified, investigated, resolved, and documented in a timely and controlled manner.

All incidents are recorded upon identification and classified according to their nature, severity, operational impact, affected systems or services, and potential regulatory significance. Incident records include, where applicable, a description of the incident, the date and time of occurrence, affected systems or business processes, actions taken, responsible personnel, investigation findings, corrective measures, and the final resolution.

Incidents are escalated according to their severity, business impact, and regulatory significance. Operational and technical incidents are assigned to the responsible technical personnel, while information security incidents are coordinated by the Chief Security Officer (CSO). Depending on the nature of the incident, additional involvement may include Operations, Customer Support, Compliance, AML, Fraud Prevention, Payment Operations, senior management, and other authorised personnel responsible for the affected business or technical functions.

The Company investigates incidents to determine their root cause, assess operational, security, and regulatory impact, implement appropriate corrective actions, and reduce the likelihood of recurrence. Significant activities performed during the incident response process are documented and retained in accordance with the Company's record retention requirements.

An incident is formally closed once the affected services have been restored, corrective actions have been completed, and the responsible personnel have confirmed that the incident has been resolved. The incident record is updated to document the outcome of the investigation, corrective actions implemented, and the formal closure of the incident. Where appropriate, post-incident reviews are performed to identify lessons learned and opportunities to strengthen operational resilience and information security controls.

Where required by applicable laws, regulatory requirements, or the Company's licence conditions, the Company notifies the Curaçao Gaming Authority of reportable incidents within the applicable regulatory timeframe. Where appropriate, the Company also communicates with affected service providers, business partners, customers, or other relevant stakeholders where such notification is necessary to support incident resolution, fulfil contractual obligations, or comply with legal or regulatory requirements.

11. TECHNICAL INFRASTRUCTURE

11.1 Hosting Environment

The Company's production platform is hosted within a secure cloud-based infrastructure provided by third-party infrastructure service providers. The hosting environment incorporates virtual networking, load balancing, containerised application services, databases, and supporting infrastructure designed to ensure the secure, reliable, and scalable delivery of the Company's gaming services.

The infrastructure is protected through multiple layers of network security and is supported by geographically separated primary and backup environments to facilitate business continuity and disaster recovery. The platform is designed with infrastructure redundancy, continuous monitoring,

secure backup arrangements, and resilience measures to support the availability and integrity of critical systems.

The Company utilises third-party cloud infrastructure and network service providers to support the operation, availability, security, and resilience of the platform.

The technical infrastructure includes cloud-hosted application services, managed databases, network load balancing, web application protection, container orchestration, monitoring and logging capabilities, backup infrastructure, and secure integrations with external service providers. A high-level architecture diagram illustrating the principal platform components, data flows, and external integrations is provided in Section 11.7 of this Manual.

11.2 Production Environment

The Company's production environment comprises the systems and infrastructure required for the delivery of licenced gaming services. The production environment includes the gaming platform, application services, databases, network and security components, monitoring and logging services, backup infrastructure, and integrations with authorised third-party service providers supporting the Company's operations.

The Company maintains separate production and non-production environments. Development, testing, validation, and quality assurance activities are performed outside the live production environment. Changes are tested prior to deployment and, where technically feasible, are first validated in a non-production environment before being released to production.

Access to the production environment is restricted to authorised personnel whose duties require such access. Access is granted in accordance with the Company's access management procedures and the principle of least privilege. Administrative access is limited to authorised technical personnel and is subject to approval, periodic review, and audit. Technical and organisational security measures, including Role-Based Access Control (RBAC), Access Control Lists (ACLs), IP allowlists, and Two-Factor Authentication (2FA), are implemented where applicable to protect the production environment.

Access to production systems is limited to authorised personnel performing technical, operational, security, or support functions where such access is required for the performance of their responsibilities. Each authorised user is granted only the permissions necessary for their assigned duties, and all activities are performed within the scope of their approved access rights. Administrative activities are logged and subject to monitoring and periodic review.

11.3 Disaster Recovery

The Company maintains a disaster recovery environment designed to support the restoration of critical systems and services following a major operational disruption, infrastructure failure, or other significant incident. The disaster recovery environment is supported by geographically separated backup infrastructure and replicated system components to facilitate the continuity of business operations.

The disaster recovery process is intended to restore the availability of critical services by redirecting operations to the disaster recovery environment where necessary, restoring system functionality, and recovering data from replicated backups. Recovery activities are coordinated by the responsible technical personnel in accordance with the Company's incident management, business continuity, and disaster recovery procedures.

The disaster recovery scope includes the gaming platform, application services, databases, network infrastructure, security services, backup systems, and other supporting technical components required to restore the Company's critical business operations following a disruption.

The Company establishes recovery objectives for critical systems and services as part of its disaster recovery arrangements. Recovery priorities are determined through business impact analysis, which identifies the systems requiring restoration and the required recovery timeframe based on operational impact and business criticality.

The disaster recovery arrangements are reviewed periodically and tested on a regular basis to verify that critical systems, personnel, and recovery procedures remain effective and capable of supporting the continuation of business operations following a significant disruption.

11.4 Business Continuity

The Company maintains a business continuity framework designed to ensure the continued availability of licenced gaming services, critical business processes, technical infrastructure, and customer support functions in the event of operational disruption, information security incidents, infrastructure failures, cyber incidents, natural disasters, or other events that may affect the continuity of operations.

The primary objective of the business continuity framework is to minimise operational disruption, protect customers, maintain regulatory compliance, preserve the integrity and availability of critical systems, and enable the timely recovery of essential business operations.

The Company has identified the following as critical business functions:

- operation of the gaming platform and production environment;
- player account management;
- payment processing, including deposits and withdrawals;
- customer support services;
- information security monitoring and incident response;
- operation of critical databases and network infrastructure;
- regulatory reporting and compliance activities.

Business continuity is supported through organisational and technical measures including:

- geographically separated primary and secondary data centres;
- replicated production infrastructure and databases;
- backup and recovery arrangements for critical systems;
- traffic redirection to secondary infrastructure where required;
- standby server infrastructure;
- secure remote access for authorised personnel;
- alternative customer communication channels;
- Business Impact Analysis (BIA) to determine recovery priorities following operational disruption.

Overall responsibility for business continuity rests with the Chief Technology Officer (CTO). Recovery activities are coordinated with Information Security, Risk Management, Operations, Customer Support, Compliance, Senior Management, and other relevant functions depending on the nature of the incident. Where required, the Chief Executive Officer (CEO) and the Board of Directors participate in strategic recovery decisions. Material incidents affecting licenced operations are reported to the Curaçao Gaming Authority in accordance with applicable regulatory requirements.

The business continuity framework is reviewed periodically and following significant operational, technological, organisational, or regulatory changes. Recovery arrangements are regularly tested through technical recovery exercises, operational simulations, and validation of restoration procedures. Test results, identified weaknesses, and corrective actions are documented and incorporated into the Company's continuous improvement process.

11.5 Monitoring and Alerting

The Company maintains a continuous monitoring and alerting framework designed to ensure the availability, security, integrity, and performance of its gaming platform, supporting infrastructure, and critical business services. Monitoring activities enable the timely detection, assessment, escalation, and resolution of operational, technical, security, and compliance-related events.

The monitoring framework covers the Company's production environment, infrastructure components, applications, network connectivity, third-party integrations, and operational processes that support the provision of licenced gaming services.

Monitoring activities include, where applicable:

- availability and performance of the gaming platform;
- availability and health of production servers, databases, and network infrastructure;
- application performance and service response times;
- payment processing services and third-party integrations;
- system capacity and resource utilisation;
- backup processes and recovery status;
- cybersecurity events, including unauthorised access attempts, malware detection, and security incidents;
- distributed denial-of-service (DDoS) protection events and network anomalies;
- customer authentication and account security events;
- AML/CFT transaction monitoring alerts;
- fraud prevention alerts and detection of unusual customer behaviour;
- system errors, application failures, and critical operational exceptions.

Monitoring information is collected through automated monitoring solutions integrated with the Company's infrastructure and operational environment. Where predefined thresholds, abnormal behaviour, or critical events are detected, alerts are generated automatically and classified according to their severity, business impact, and operational priority.

Critical alerts are immediately escalated to the responsible operational teams. Depending on the nature of the event, notifications may be assigned to the Technical Department, Information Security, Payment Operations, Compliance, AML, Fraud Prevention, Customer Support, or other responsible business functions. Major incidents are escalated to senior management in accordance with the Company's Incident Management procedures.

The Company operates continuous twenty-four (24) hour monitoring of critical production systems and security controls to support the uninterrupted provision of gaming services. Monitoring activities include both automated monitoring and operational oversight by authorised personnel to ensure that material incidents are identified and addressed without undue delay.

Monitoring events, alerts, incident records, escalation actions, and remediation activities are retained in accordance with the Company's record retention, information security, and regulatory requirements.

11.6 Change Management

The Company maintains a formal Change Management process to ensure that modifications to systems, applications, infrastructure, security controls, and operational processes are implemented in a controlled manner while minimising operational, technical, and information security risks.

All changes are initiated by the relevant business or technical functions in response to business requirements, regulatory obligations, security improvements, incident remediation, system enhancements, infrastructure optimisation, or third-party integration requirements. Prior to implementation, each proposed change is assessed for its potential impact on system availability, information security, operational continuity, regulatory compliance, and customer experience.

Changes are reviewed and approved by authorised personnel according to their nature, complexity, and level of risk. Depending on the scope of the proposed change, the approval process may involve the Chief Technology Officer (CTO), the Chief Security Officer (CSO), who performs the Company's information security function, the Compliance function, and the managers of the relevant business or technical departments.

The Company classifies changes according to their operational impact and associated risk. Changes with a higher risk profile or those affecting critical systems, security controls, or licenced operations are subject to enhanced assessment, approval, testing, and post-implementation review.

All changes are tested prior to deployment into the production environment. Testing may include functional testing, integration testing, security validation, performance testing, regression testing, and user acceptance testing, where appropriate. Whenever technically feasible, changes are first deployed and validated in a non-production environment before being released into the live production environment.

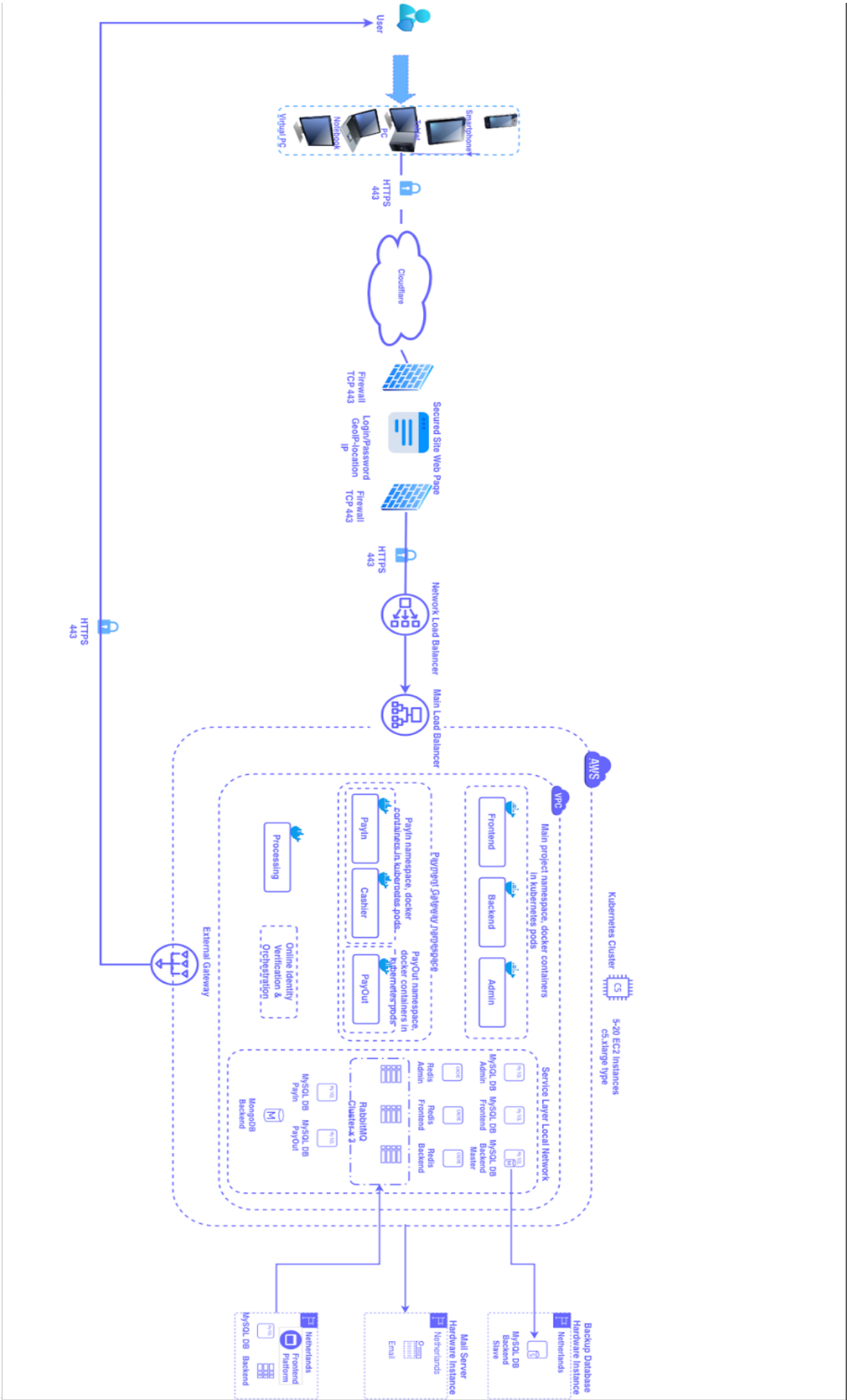
All implemented changes are documented and recorded. Change documentation includes the purpose and description of the change, risk assessment, approvals obtained, testing performed, implementation date, responsible personnel, and implementation outcome. Following deployment, the affected systems are monitored to verify successful implementation, identify any unexpected issues, and ensure the continued availability, integrity, performance, and security of the Company's licenced gaming services. Where necessary, rollback procedures are available to restore the previous stable configuration.

11.7 Platform Architecture Diagram (Internal)

The technical infrastructure diagram provides a high-level overview of the Company's production platform architecture and identifies the principal infrastructure components supporting the licenced gaming operation. The diagram illustrates the hosting environment, network security controls, application services, databases, payment services, external integrations, load balancing, firewalls, messaging services, backup and redundancy mechanisms, and other critical platform components.

The diagram also depicts the logical data flows between systems and identifies the locations where player information, transaction records, gaming data, and other operational information are processed and securely stored. It is maintained as an internal controlled document and is reviewed and updated following material changes to the Company's infrastructure or system architecture.

High-Level Platform Architecture (Internal)



12. RECORD KEEPING

12.1 Gaming Records

The Company maintains records of gaming activity generated through the operation of its products and services.

Gaming records may include:

- gaming sessions;
- bets placed by customers;
- game rounds;
- game outcomes;
- winnings and losses;
- cancelled or voided bets;
- interrupted or incomplete gaming sessions;
- jackpot participation and payouts;
- bonus-related gaming activity;
- balance adjustments resulting from gaming activity;
- timestamps associated with gaming events and transactions;
- game identifiers and transaction references;
- other records required to support operational, regulatory, financial, compliance, dispute resolution, and audit requirements.

Gaming records are maintained to support customer account management, financial reconciliation, complaint handling, dispute resolution, regulatory reporting, fraud prevention, AML/CFT controls, and internal audit activities.

12.2 Customer Records

The Company maintains customer records necessary for the establishment, administration, monitoring, and termination of customer relationships.

Customer records may include:

- customer registration information;
- personal identification data;
- contact details;
- account information;
- account status history;
- customer verification records;
- identity documents;
- proof of address documentation;
- payment method information;
- customer communications;

- customer support interactions;
- account restriction records;
- account suspension records;
- account closure records;
- responsible gaming records;
- consent and preference records;
- risk assessment records;
- customer declarations and confirmations;
- other records required for operational, regulatory, compliance, legal, or audit purposes.

Customer records are maintained to support customer onboarding, account administration, customer verification, responsible gaming controls, fraud prevention measures, AML/CFT compliance, complaint handling, regulatory reporting, and internal governance processes.

12.3 Financial Records

The Company maintains financial records relating to customer transactions and financial operations performed through the platform.

Financial records may include:

- deposit transactions;
- withdrawal transactions;
- payment method information;
- payment transaction statuses;
- cancelled transactions;
- reversed transactions;
- rejected transactions;
- chargebacks;
- refunds;
- bonus credits and bonus deductions;
- manual balance adjustments;
- account balance movements;
- payment processing records;
- financial reconciliation records;
- transaction references and identifiers;
- timestamps associated with financial transactions;
- records supporting regulatory, accounting, compliance, audit, and operational requirements.

Financial records are maintained to support payment processing, financial reconciliation, customer account administration, complaint handling, regulatory reporting, AML/CFT compliance, accounting activities, and internal audit functions.

12.4 AML Records

The Company maintains AML/CFT records to demonstrate compliance with applicable legal, regulatory, and internal AML/CFT requirements.

AML records may include:

- Customer Due Diligence (CDD) records;
- Enhanced Due Diligence (EDD) records;
- Know Your Customer (KYC) documentation;
- identity verification records;
- proof of address documentation;
- Source of Funds (SoF) documentation;
- Source of Wealth (SoW) documentation;
- customer risk assessments;
- AML risk classification records;
- ongoing monitoring records;
- transaction monitoring alerts;
- sanctions screening results;
- PEP screening results;
- adverse media screening results;
- internal AML investigations;
- unusual activity reviews;
- suspicious activity assessments;
- SAR/STR related records and supporting documentation;
- communications relating to AML reviews;
- account restriction decisions related to AML/CFT controls;
- account suspension decisions related to AML/CFT controls;
- account closure decisions related to AML/CFT controls;
- regulatory correspondence relating to AML/CFT matters;
- AML training records;
- AML audit and review records;
- other records required to support AML/CFT compliance obligations.

AML records are maintained to support customer due diligence, ongoing monitoring, sanctions compliance, suspicious activity reporting, regulatory reporting, internal investigations, audit activities, and regulatory inspections.

12.5 Retention Periods

The Company retains records in accordance with applicable legal, regulatory, AML/CFT, accounting, operational, and business requirements.

Records maintained by the Company include, but are not limited to, gaming records, customer records, financial records, AML/CFT records, customer verification documentation, sanctions screening records, complaint records, audit records, and other operational records generated in the course of business activities.

Unless a longer retention period is required by applicable law, regulatory obligation, court order, ongoing investigation, audit, or other legitimate business purpose, records maintained by the Company are retained for a minimum period of five years.

Where records are subject to regulatory inquiries, investigations, litigation, enforcement actions, audit activities, or other legal preservation requirements, the Company may extend the retention period until the relevant matter has been fully resolved.

Upon expiry of the applicable retention period, records may be archived, anonymised, or securely destroyed in accordance with the Company's internal procedures and applicable legal and regulatory requirements.

The Company applies appropriate administrative, technical, and organisational measures to ensure the integrity, availability, confidentiality, and accessibility of retained records throughout the applicable retention period.

12.6 Server and Data Center Requirements

In compliance with applicable regulatory requirements, the digital records kept of specific critical information about players, their gaming transactions, and their financial transactions are maintained and kept available to the Curaçao Gaming Authority (CGA) at all times. These critical records are stored on a server located in a Tier-IV certified data center registered in Curaçao (such as Blue Nap Americas or another equally certified and licenced infrastructure provider within the jurisdiction).

The Company selects its data center partners based on strict security, resilience, and compliance criteria. Evidence confirming the selected data center's Tier-IV certification and local corporate registration is maintained by the Legal Department and will be made available to the CGA upon request.

13. REGULATORY REPORTING

13.1 Amendment Reports

The Company maintains records of amendments made to the Operations Manual and other regulatory documentation. Updated versions of relevant documents are submitted to the regulator in accordance with applicable reporting requirements.

13.2 Incident Reports

The Company maintains procedures for documenting and reporting material incidents affecting the operation of the business. Such incidents may include security breaches, system failures, gaming-related fraud, criminal activity, or other events requiring notification to the regulator.

13.3 Transaction Reports

The Company maintains records and reporting processes relating to customer transactions and other reportable financial activities. Transaction reports are prepared and submitted where required by applicable regulatory or AML/CFT requirements.

13.4 Complaints and ADR Reports

The Company maintains records of customer complaints, disputes, and dispute resolution outcomes. Information may be compiled and reported to competent authorities where required.

13.5 Change and Independent Expert Reports

The Company maintains records of material operational changes and independent assessments relating to regulatory compliance. Reports may include changes to the operational structure of the business as well as assessments performed by independent experts in areas such as system controls, responsible gaming, AML/CFT compliance, and other regulatory requirements.

13.6 Communication with the Authority

The Managing Director holds the primary access to the CGA portal. All official requests for information, documentation, and regulatory inquiries logged by the Curaçao Gaming Authority are received, managed, and coordinated through this access to ensure timely, accurate, and compliant regulatory responses.

14. TRAINING AND AWARENESS

14.1 Annual Training

The Company maintains an annual training programme to ensure that employees remain aware of their compliance, operational and regulatory responsibilities. Training content is reviewed periodically and updated to reflect changes in legislation, regulatory expectations, internal procedures, products, services and identified risks.

14.2 AML Training

The Company provides AML/CFT/CPF training to employees whose duties may expose them to money laundering, terrorist financing or proliferation financing risks. Training is provided upon hiring and periodically thereafter. The programme is designed to help employees identify suspicious activity, understand customer due diligence requirements, follow internal reporting procedures and fulfil their AML obligations.

14.3 Responsible Gaming Training

The Company provides Responsible Gaming training to relevant employees to support the identification of customers who may be experiencing gambling-related harm. The training covers responsible gaming principles, customer interaction standards, self-exclusion measures, account restrictions and escalation procedures.

14.4 Information Security Training

The Company provides Information Security training to employees to promote the secure handling of customer information, company assets and confidential data. The training includes cyber security awareness, password management, phishing prevention, data protection requirements and incident reporting procedures.

14.5 Training Records

The Company maintains records of all training activities, including attendance records, training materials, assessment results and completion dates. Training records are retained in accordance with the Company's record retention procedures and applicable legal and regulatory requirements.