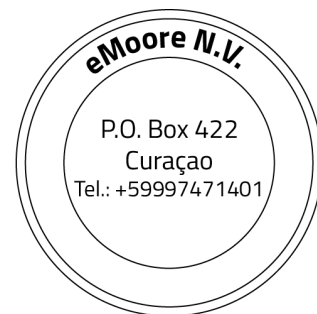


OPERATIONAL MANUAL

DIGIBET NV

Signature: *C. Drommond*
Name: C. Drommond, Proxyholder of eMoore N.V.
Date: June 30, 2026



Version: 1.0

Effective Date: 30.06.2026

Prepared By: internal Compliance Department

Approved By: Director, eMoore N.V.

Confidentiality Classification: Internal & Regulatory Use Only

TABLE OF CONTENTS

1. Introduction
2. Corporate Overview
3. Description of Games of Chance
4. Payment Methods and Financial Flows
5. Software and Outcome Determination
6. Quality Monitoring and Testing Procedures
7. Data Protection and Player Information Storage
8. Player Interface and Visual Elements
9. Prevention of Access by Vulnerable and Excluded Persons
10. Technical Infrastructure and Business Continuity
11. Responsible Gaming Measures
12. Terms and Conditions
13. Player Complaints and Dispute Resolution
14. Digital Recordkeeping and Financial Data Retention
15. Internal Controls and Governance
16. Incident Reporting and Escalation
17. Appendices

1. INTRODUCTION

This Operational Manual describes the operational, technical, compliance, responsible gaming, and governance procedures implemented by DIGIBET NV (the “License Holder”) in connection with its online Games of Chance operations conducted under the Curaçao Landsverordening op de Kansspelen (“LOK”).

This manual is intended to demonstrate compliance with:

- Curaçao gaming legislation;
- Applicable ministerial regulations;
- Conditions attached to the License Holder’s gaming license;
- AML/CFT legislation;
- Data protection obligations;
- Responsible gaming obligations; and
- Applicable technical and operational standards.

This manual applies to all gaming operations conducted through the License Holder’s approved URLs, domains, software applications, and related operational infrastructure.

2. CORPORATE INFORMATION

2.1 Legal Entity Details

Digibet NV

Registration Number Chamber of Commerce: **158812**

Registered Address: Groot Kwartierweg 10, Livestrong building, Curaçao

Website(s)/URL(s):

www.goalbet.com,

www.racetan.com,

www.betbetty.com,

www.kingonbet.com,

www.maxbetonwin.com

2.2 Shareholding structure and infrastructure

The License Holder maintains an up-to-date register of:

- Shareholders;
- Ultimate Beneficial Owners (UBOs);
- And Directors;

All changes are reported to the Curaçao Gaming Authority in accordance with applicable requirements.

In addition to corporate records, the License Holder shall maintain an up-to-date register of its technical infrastructure, including:

- Core platform architecture and system components;
- Hosting environments, including cloud service providers and data center locations;
- Critical systems such as gaming platforms, wallet systems, and databases;
- Network architecture, including security layers and access controls;
- Third-party service providers involved in infrastructure, hosting, or system operations;
- and
- Backup, redundancy, and disaster recovery configurations.

Such records shall ensure full visibility of the operational environment and support effective risk management, security oversight, and regulatory compliance. A copy of this infrastructure is **Appendix A**.

3. DESCRIPTION OF THE GAMES OF CHANCE

3.1 Categories of Games Offered

The License Holder offers the following Games of Chance:

Casino Games

Slots: Digital reel-based games where players spin to match symbols and win prizes based on predefined paylines or bonus features.

Roulette: A wheel-based game where players wager on where a ball will land, including numbers, colors, or combinations.

Blackjack: A card game where players compete against the dealer to achieve a hand value closest to 21 without exceeding it.

Baccarat: A card game where players bet on the outcome of the Player or Banker hand, or a tie.

Live Casino Games: Real-time casino games streamed from studios or gaming facilities, featuring live dealers and interactive gameplay.

Betting Products

Sports Betting: Wagering on the outcome of sporting events across various markets, including match results, scores, and player performance.

In-Play Betting: Real-time betting during live sporting events with dynamically updated odds.

Virtual Sports: Computer-generated sporting events with randomized outcomes available for continuous betting.

Additional Gambling Products

Lottery Games: Games where players purchase entries for a chance to win prizes based on random draws.

Instant Win Games: Fast-play games where results are determined immediately, including scratch cards or digital equivalents.

Bingo Games: Number-based games where players match drawn numbers on cards to achieve predetermined winning patterns.

Keno: A lottery-style game where players select numbers and win based on matches with randomly drawn numbers.

Crash Games: Multiplayer games where players attempt to cash out before a rising multiplier crashes, combining chance and timing decisions.

Jackpot Games: Games featuring progressive or fixed jackpots that accumulate until won.

Other Approved Gaming Products: Any additional gaming products approved by the relevant regulatory authority under applicable legislation.

An overview of all Games of Chance offered by the License Holder can be found as **Appendix B**.

3.2 Game Rules and Participation Conditions

The rules applicable to each game shall:

- Be published on the License Holder's gaming website(s);
- Be made available to players prior to their participation in any game; and
- Be accessible in the English language and, where applicable, in any additional languages supported by the License Holder.
-

Such rules shall, at a minimum, include clear and comprehensive provisions specifying:

- The applicable minimum and maximum stake limits;
- The conditions governing the determination of winning outcomes;
- Any terms, limitations, or restrictions applicable to bonuses or promotional offers;
- The procedures governing the validation and settlement of bets; and
- The circumstances under which wagers may be deemed void, cancelled, or otherwise invalid.

The License Holder shall ensure that all game rules are transparent, accurate, and readily accessible at all times to ensure fair play and informed participation.

3.3 Bet Amounts

The License Holder shall implement and maintain appropriate controls to ensure that all betting limits are defined, enforced, and monitored in accordance with regulatory requirements, risk management principles, and player protection objectives.

Betting limits shall be configured on a per-game and per-product basis and may vary depending on a range of factors, including:

- Risk management settings, reflecting the License Holder's internal risk tolerance, exposure limits, and trading strategies;
- Jurisdictional restrictions, ensuring compliance with applicable legal and regulatory requirements in the jurisdictions where services are offered;
- Player account status, including verification level, risk profile, and any applicable account restrictions or enhancements; and
- Currency denomination, taking into account differences in value and conversion rates across supported currencies.

The License Holder shall ensure that all betting limits are clearly defined within the relevant game configurations and are consistently applied across all channels and platforms.

Automated controls shall be implemented to:

- Prevent players from placing wagers outside the configured minimum and maximum thresholds;
- Enforce all applicable regulatory and operational limits in real time; and
- Detect and block any attempts to circumvent established wagering controls.

Such controls shall form part of the broader system integrity framework and shall be subject to regular testing, monitoring, and review to ensure ongoing effectiveness and compliance.

Any changes to betting limits shall be subject to formal configuration management and approval processes, with appropriate audit trails maintained to ensure transparency and traceability.

3.4 Payouts and Return-to-Player (RTP)

Payouts and game outcomes shall be determined using fair, transparent, and independently verified systems and processes, including certified Random Number Generator (RNG) systems, approved sports odds engines, approved live dealer systems, official data feeds from licensed providers, and certified game logic in accordance with applicable regulatory requirements.

All systems used in determining outcomes and payouts shall be subject to independent testing, certification, and periodic verification by approved testing laboratories or competent regulatory authorities to ensure compliance with recognized standards of fairness, integrity, and reliability.

The applicable Return to Player (RTP) percentages shall be predefined within certified game configurations and shall comply with regulatory thresholds, remain unchanged without proper authorization and re-certification, and be disclosed to players where required.

The License Holder shall maintain effective controls to ensure accurate payout calculations, system integrity, protection against manipulation or unauthorized interference, and timely identification and resolution of any system malfunctions or irregularities. Affected games shall be suspended where necessary to protect players and maintain fairness.

The License Holder shall establish and maintain robust audit and compliance frameworks to ensure adherence to all applicable legal and regulatory obligations.

This shall include maintaining complete, accurate, and tamper-evident records of all transactions, outcomes, and payout calculations, as well as retaining audit logs and system data in accordance with regulatory requirements.

Internal audit procedures shall be implemented to periodically assess the effectiveness of controls governing game integrity, payout accuracy, and system security.

Independent external audits and certifications shall be conducted by accredited testing laboratories or qualified third parties at regular intervals.

The License Holder shall provide regulators with access to relevant records, systems, and documentation upon request to verify compliance.

Any material system failures, integrity breaches, or discrepancies affecting outcomes or payouts shall be promptly reported to the relevant regulatory authority in accordance with applicable reporting timelines.

Corrective and preventive actions shall be implemented to address any deficiencies or non-compliance identified. All systems, controls, and processes shall remain fully compliant with applicable Curaçao gaming legislation (LOK) and any directives or technical standards issued by the competent authority.

3.5 Software Providers

Gaming software deployed by the License Holder shall be sourced from approved and certified software providers. The License Holder shall implement and maintain a robust governance framework to ensure that all third-party software providers are subject to appropriate due diligence, risk assessment, and ongoing oversight. This includes verifying that providers:

- Hold valid licenses or approvals in recognized jurisdictions;
- Maintain relevant certifications issued by accredited independent testing laboratories (e.g., for RNG integrity, game fairness, and system security); and

- Adhere to applicable standards relating to data protection, cybersecurity, and operational resilience.

The License Holder shall maintain comprehensive, accurate, and current records in respect of all software providers and their products, including but not limited to:

- The legal name, registration details, and corporate structure of each provider;
- The jurisdictions in which the provider is licensed, regulated, or otherwise authorized to conduct gaming-related activities;
- Certification reports, test results, and approval documentation relating to each game or software component;
- Version control information, including software release history, updates, patches, and any modifications affecting game logic or functionality;
- Integration and implementation records, including system testing results, acceptance criteria, and deployment approvals; and
- Details of any subcontractors or critical dependencies involved in the delivery of the software services.

All records shall be maintained in a secure, structured, and auditable manner to ensure full traceability of software deployment and changes throughout the system lifecycle. Such records must be readily accessible and available for inspection by the relevant regulatory authority upon request.

The License Holder shall further ensure that:

- Any software updates, patches, or changes are subject to formal change management procedures, including testing, approval, and, where applicable, re-certification prior to deployment;
- Continuous monitoring is performed to detect any anomalies, malfunctions, or integrity issues associated with third-party software;
- Appropriate contractual arrangements are in place with software providers, clearly defining responsibilities, service levels, compliance obligations, and audit rights; and
- Any incidents, defects, or vulnerabilities identified in relation to third-party software are promptly escalated, investigated, and resolved in accordance with the License Holder's incident management and regulatory reporting procedures.

Periodic reviews shall be conducted to assess the ongoing suitability, performance, and compliance status of all software providers. Where deficiencies or non-compliance are identified, the License Holder shall implement appropriate corrective actions, including suspension or replacement of the relevant provider where necessary.

An overview of all software providers engaged by the License Holder, including relevant licensing jurisdictions, certifications, and products supplied, is set out in **Appendix C**.

3.6 Outcome Determination

Game outcomes shall be determined exclusively through secure, automated, and independently verified mechanisms, including:

- Independently certified Random Number Generator (“RNG”) systems, ensuring that outcomes are random, unbiased, and not susceptible to prediction or manipulation;
- Official sports data providers, supplying accurate, verified, and timely event data for the settlement of sports wagers; and
- Algorithmic settlement engines, applying predefined rules and logic to ensure consistent, accurate, and auditable bet settlement processes.

Under no circumstances shall manual intervention be permitted in the determination, manipulation, or alteration of game outcomes. All outcome processes shall be fully automated and governed by certified systems and approved game logic.

The License Holder shall implement and maintain appropriate technical and operational controls to ensure the integrity of all outcome determination processes, including:

- The prevention of unauthorized access to systems responsible for outcome generation and settlement;
- Continuous monitoring for anomalies, irregular patterns, or potential integrity breaches;
- The immediate investigation and remediation of any identified system errors or inconsistencies.

All systems and processes involved in determining game outcomes shall be subject to independent testing, certification, and periodic audit to ensure compliance with applicable regulatory requirements and recognized industry standards.

Records of game outcomes and settlement activities shall be securely maintained to ensure full traceability, auditability, and availability for regulatory inspection.

4. PAYMENT METHODS AND FINANCIAL OPERATIONS

4.1 Accepted Payment Methods

The License Holder may offer and accept a range of payment methods, subject to regulatory approval and applicable legal requirements, including credit and debit cards, bank transfers, electronic wallets, cryptocurrency (where permitted), and other approved methods. All payment methods shall be provided through authorized and reputable payment service providers and integrated securely. An overview is provided in **Appendix D**.

4.2 Deposit Procedures

Deposits shall only be accepted from identified player accounts. Controls include KYC verification, fraud monitoring, AML/CFT screening, velocity checks, and verification of payment method ownership. All deposit activities shall be monitored in accordance with the AML Policy of the License Holder.

4.3 Withdrawal Procedures

Withdrawals shall be processed to verified payment methods, subject to fraud checks, AML/CFT controls, and internal policies. Requests exceeding thresholds shall undergo enhanced due diligence and manual review. Withdrawals shall be processed accurately and within reasonable timeframes.

4.4 Segregation and Safeguarding of Player Funds

Player funds shall be administratively segregated from operational funds. Daily reconciliations must be performed to verify balances and identify discrepancies. Records shall be maintained for audit and regulatory inspection.

5. SOFTWARE AND OUTCOME DETERMINATION

5.1 Gaming Platform

The License Holder operates a fully integrated and scalable gaming platform designed to support licensed gaming services in a secure, reliable, and compliant manner. The platform includes a front-end player interface, wallet system, bonus engine, risk engine, reporting systems, and administrative backend. All components are developed in accordance with secure development principles and are subject to testing, validation, and change management prior to deployment. The platform supports high availability, redundancy, and operational continuity. Documentation of architecture, system dependencies, and data flows is maintained for audit and regulatory purposes.

5.2 Core Components

Front-End Player Interface: Provides secure player access to gaming services.

Wallet System: Manages player balances and transactions.

Bonus Engine: Controls promotional offers and wagering requirements.

Risk Engine: Monitors player behavior for fraud and suspicious activity.

Reporting Systems: Generates operational and regulatory reports.

Administrative Backend: Enables system configuration and account management by authorized personnel.

5.3 Technical Security

The License Holder maintains a comprehensive information security framework to protect systems and data. Security measures include encryption of data in transit and at rest, web application firewalls, DDoS protection, multi-factor authentication, role-based access control, and continuous

monitoring. Access to critical systems is logged and auditable. Security testing such as vulnerability assessments and penetration tests are conducted regularly. Patch management processes ensure systems remain protected against known vulnerabilities.

5.4 Additional Controls

Security incidents are managed in line with incident management procedures. Backup and disaster recovery mechanisms ensure system restoration. Third-party integrations undergo security assessments. All controls align with industry standards such as ISO 27001 and comply with Curaçao LOK regulatory requirements. Regular internal and external audits are conducted to validate effectiveness and compliance.

6. QUALITY MONITORING AND TEST METHODS

6.1 Testing Procedures

The License Holder shall implement and maintain comprehensive testing and monitoring procedures to ensure the integrity, security, and reliability of all gaming operations and supporting systems.

- RNG integrity
- System availability
- Payment processing
- Wallet functionality
- Access controls
- Security vulnerabilities
- Responsible gaming systems

6.2 Independent Testing

Critical gaming systems shall be independently tested and certified by accredited testing laboratories.

- RNG certification
- Penetration testing
- Security audits
- Source code review
- Fairness verification

6.3 Monitoring Frequency

Monitoring Activity

Vulnerability Scans

Penetration Tests

Backup Restoration Testing

Minimum Frequency

Monthly and after major changes

At least annually or after significant changes

Quarterly

Disaster Recovery Testing	Annually
Access Control Reviews	Quarterly
System Availability Monitoring	Continuous (24/7)
Transaction Monitoring	Continuous
Responsible Gaming Monitoring	Continuous

7. STORAGE OF PLAYER PERSONAL DATA

7.1 Personal Data Collected

The License Holder shall collect and process personal data strictly in accordance with applicable legal, regulatory, and operational requirements.

- Identification data
- Contact information
- Date of birth
- Payment information
- Transaction records
- Gaming activity
- Device and IP information
- KYC documentation

7.2 Data Storage and Security

Personal data shall be stored securely using appropriate technical and organizational measures.

- Encrypted databases
- Secure hosting environments
- Role-based access controls

Encryption shall be applied to:

- Data in transit
- Data at rest
- Backup storage

7.3 Data Retention

Data retention shall comply with applicable legal and regulatory requirements.

- Curaçao legal requirements
- AML/CFT obligations
- Regulatory recordkeeping obligations

Archived records shall remain retrievable for regulatory review.

7.4 Access Logging and Control

Administrative access to personal data shall be controlled and monitored.

- Logged
- Monitored
- Restricted to authorized personnel

8. PLAYER-FACING VISUAL ELEMENTS

8.1 Website and Application Disclosures

The License Holder ensures that the gaming website and applications provide clear, accurate, and accessible information to players.

- Account balances
- Active bonuses
- Betting history
- Responsible gaming tools
- Terms and Conditions
- Privacy notices
- Regulatory notices

8.2 Responsible Gaming Notices

The following notices are prominently displayed on the websites:

- Minimum age restrictions
- Responsible gaming messages
- Self-exclusion information
- Player support resources

For detailed information regarding the Company's Responsible Gaming procedures, please refer to the attached Responsible Gaming Policy, which is provided as a separate document.

8.3 User Interface Controls

The player interface includes tools designed to support responsible gaming:

- Deposit limit tools
- Session reminders
- Cooling-off functionality
- Account closure requests
- Reality check notifications

9. PREVENTION OF ACCESS BY VULNERABLE OR EXCLUDED PERSONS

9.1 Age Verification Measures

The License Holder shall strictly prohibit access to its gaming services by individuals below the legal minimum age of 18 years, or such higher age as may be required by applicable law.

To ensure compliance with age restriction requirements, the License Holder shall implement robust verification measures, including but not limited to:

- Know Your Customer (“KYC”) procedures to confirm player identity and age;
- Verification of identification documents issued by recognized authorities;
- Automated age validation systems integrated within onboarding processes; and
- Screening against third-party databases and verification services, where applicable.

Access to gaming services shall not be granted until sufficient verification has been successfully completed. The License Holder shall maintain records of all verification activities for audit and regulatory purposes.

9.2 Self-Exclusion Procedures

The License Holder shall provide players with the ability to voluntarily restrict their access to gaming services through a range of self-exclusion options.

Players may request:

- Temporary self-exclusion for a defined period;
- Permanent self-exclusion resulting in indefinite account closure; and
- Cooling-off periods designed to provide short-term breaks from gaming activity.

Players who are subject to self-exclusion measures shall be prevented from:

- Accessing or logging into their accounts;
- Depositing or transferring funds;
- Participating in any gaming activities; and
- Receiving marketing or promotional communications.

The License Holder shall ensure that self-exclusion requests are implemented promptly, consistently enforced, and maintained in accordance with regulatory requirements.

9.3 Vulnerable Player Detection

The License Holder shall implement both automated systems and manual oversight processes to identify potential indicators of problematic or high-risk gambling behavior.

Monitoring mechanisms shall assess player activity and behavioral patterns, including but not limited to:

- Excessive or increasing deposit activity;
- Rapid or repetitive wagering behavior;
- Extended or continuous gaming sessions;
- Repeated failed deposit attempts or unusual payment patterns; and
- Other behavioral markers indicative of potential gambling-related harm.

Such monitoring shall be conducted on an ongoing basis, supported by risk-based thresholds and alert systems designed to facilitate early identification and intervention. In **APPENDIX E** the technical measures that are put in place to prevent admission are mentioned.

9.4 Intervention Measures

Where indicators of vulnerable or problematic gambling behavior are identified, the License Holder shall implement appropriate and proportionate intervention measures to mitigate risk and protect the player.

Such interventions may include:

- The provision of responsible gaming messaging and on-screen notifications;
- Direct communication with the player, including proactive outreach by trained personnel;
- The application of account-based limitations, including deposit, wagering, or session restrictions;
- The imposition of mandatory cooling-off periods; and
- The application of enforced or permanent exclusion measures where necessary.

All intervention actions shall be documented and subject to review to ensure effectiveness and consistency with responsible gaming obligations.

For further details, reference is made to the License Holder's Responsible Gaming Policy, which sets out the full framework governing player protection, monitoring, and intervention procedures.

10. TECHNICAL INFRASTRUCTURE AND BUSINESS CONTINUITY

10.1 Infrastructure Overview

The License Holder operates a secure and resilient technical infrastructure to support continuous operations and regulatory compliance, which pertains to:

- Application servers
- Database servers
- Wallet systems
- Security infrastructure
- Cloud hosting
- Monitoring systems
- Backup systems

10.2 Infrastructure Diagram

The diagram shall include:

- Hosting architecture
- Data flows

- Security layers
- Payment gateway integrations
- Backup infrastructure
- Redundancy architecture

(Refer to Appendix A.)

10.3 Business Continuity Plan (BCP)

The License Holder maintains a Business Continuity Plan addressing key disruption scenario.

- Cybersecurity incidents
- Data corruption
- Hosting outages
- Payment interruptions
- System failures

For detailed information regarding the Company's Business Continuity Plan, please refer to the attached Business Plan, which is provided as a separate document.

10.4 Disaster Recovery

Disaster recovery measures include the following:

- Geographic redundancy
- Automated backups
- Failover systems
- Recovery testing

11. RESPONSIBLE GAMING IMPLEMENTATION

11.1 Responsible Gaming Policy

The License Holder shall establish, implement, and maintain a comprehensive Responsible Gaming Policy forming an integral part of its governance and compliance framework. The policy defines the License Holder's commitment to player protection, outlines procedures for identifying and supporting vulnerable players, and ensures compliance with Curaçao gaming legislation (LOK). The policy is subject to periodic review and approval by senior management.

11.2 Responsible Gaming Tools

Players have access to the following responsible gaming tools:

- Deposit limits
- Loss limits
- Wager limits
- Session limits

- Self-exclusion tools
- Cooling-off functionality

All tools are designed to be easily accessible, enforceable, and subject to monitoring and periodic review to ensure effectiveness.

11.3 Staff Training

The License Holder ensures that all relevant personnel receive ongoing responsible gaming training at onboarding and at least annually thereafter, regarding:

- Identification of problem gambling indicators
- Responsible gaming obligations
- Escalation procedures
- Handling of vulnerable player interactions
- Training records are maintained for audit and regulatory inspection.

11.4 Marketing Restrictions

- Marketing practices must comply with responsible and regulatory standards:
- Must not target minors
- Must not be misleading or deceptive
- Must include responsible gaming messaging
- Must not promote excessive gambling

12. TERMS AND CONDITIONS

The most recent version of the Terms and Conditions shall be maintained and made available in a manner that ensures transparency, accessibility, and compliance with applicable regulatory requirements.

The Terms and Conditions shall:

- Be published on the License Holder's gaming website;
- Be made readily accessible to players prior to account registration and participation in any gaming activities; and
- Be subject to formal version control procedures, ensuring that all updates, amendments, and historical versions are properly recorded and traceable.

The Terms and Conditions shall, at a minimum, include clearly defined provisions relating to:

- Player eligibility criteria, including age and jurisdictional restrictions;
- Account registration, usage rules, and player responsibilities;
- Bonus terms and conditions, including wagering requirements and restrictions;

- Withdrawal rules and procedures, including verification requirements and processing conditions;
- Dormant or inactive account policies, including applicable fees or handling procedures; and
- Dispute resolution procedures, including escalation channels and timelines.

A copy of the current Terms and Conditions is provided in **Appendix F**.

The License Holder acknowledges that the current Terms and Conditions will be reviewed and updated to ensure full alignment with the applicable guidelines issued by the Curaçao Gaming Authority (“CGA”). Any required amendments shall be implemented no later than 30 September 2026, in accordance with regulatory expectations.

13. PLAYER DISPUTE RESOLUTION PROCESS

13.1 Complaint Submission

The License Holder shall establish and maintain effective and accessible channels through which players may submit complaints in a timely and efficient manner, in accordance with its internal Player Complaint Policy.

Players may submit complaints through the following communication channels:

- Email communication to designated support addresses;
- Live chat functionality available on the gaming website or application; and
- A dedicated support portal or ticketing system, where available.

All complaint submission channels shall be clearly disclosed to players and remain easily accessible at all times. Further details regarding complaint submission procedures, including required information and response timelines, are set out in the License Holder’s Player Complaint Policy.

13.2 Internal Review Process

All complaints received by the License Holder shall be handled in a structured, transparent, and consistent manner, in accordance with the procedures defined in the Player Complaint Policy.

Upon receipt, each complaint shall be:

1. Formally logged within the License Holder’s complaint management system;
2. Assigned a unique reference or ticket number to ensure full traceability;

3. Acknowledged within a reasonable timeframe;
4. Investigated by appropriately qualified personnel, taking into account all relevant information, system logs, and supporting documentation; and
5. Resolved at the earliest possible opportunity or escalated where necessary.

The License Holder shall ensure that all investigations are conducted fairly, impartially, and in line with documented internal procedures and regulatory obligations.

13.3 Escalation

Where a complaint cannot be resolved to the satisfaction of the player through the internal review process, the player shall have the right to escalate the matter in accordance with the escalation procedures outlined in the Player Complaint Policy.

Escalation options shall include:

- Referral to approved alternative dispute resolution (“ADR”) mechanisms or independent adjudication bodies, where applicable; and
- Escalation to senior management, including the Managing Director or other designated senior representative of the License Holder.

The License Holder shall:

- Provide clear guidance to players on how to escalate complaints;
- Cooperate fully with any external dispute resolution processes; and
- Ensure that escalated complaints are handled in a timely and transparent manner.

13.4 Recordkeeping

The License Holder shall maintain comprehensive and auditable records of all complaints, investigations, communications, and outcomes, in accordance with applicable regulatory requirements and the provisions of the Player Complaint Policy.

Such records shall:

- Be securely stored in digital form within the License Holder’s systems;
- Contain sufficient detail to demonstrate the full lifecycle of each complaint; and
- Be retained for the duration required under applicable laws, regulations, and internal policies.

The Player Complaint Policy further defines the classification of complaints, including the criteria for identifying Reportable Complaints, as well as any associated regulatory reporting obligations. All complaint-related records shall be made available to the relevant regulatory authority upon request for the purposes of audit, inspection, or investigation.

14. DIGITAL RECORDKEEPING

14.1 Records Maintained

The License Holder shall maintain comprehensive, accurate, and up-to-date records of all operational, financial, and compliance-related activities in accordance with applicable legal and regulatory requirements.

The records maintained shall include, but are not limited to:

- Player registration data, including account details and onboarding information;
- Know Your Customer (“KYC”) documentation and due diligence records;
- Transaction histories, including deposits, withdrawals, and payment activities;
- Betting activity, including wagers placed, outcomes, and associated game data;
- Audit logs capturing system access and operational activity;
- Complaint records, including all related communications and resolutions; and
- Anti-Money Laundering and Counter-Terrorist Financing (“AML/CFT”) monitoring records, including alerts, investigations, and reporting outcomes.

All records shall be maintained in a structured and secure manner, ensuring completeness, accuracy, and traceability for audit and regulatory inspection purposes.

14.2 Security of Records

The License Holder shall implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of all records.

Such measures shall include:

- **Encryption**, to protect data both in transit and at rest against unauthorized access;
- **Robust backup procedures**, ensuring the regular and secure replication of critical data and the ability to restore records in the event of data loss;
- **Immutable logging mechanisms**, where applicable, to prevent unauthorized alteration or deletion of critical records; and
- **Access controls**, including role-based access restrictions to ensure that records are only accessible to authorized personnel on a need-to-know basis.

The License Holder shall also implement monitoring mechanisms to detect unauthorized access, data breaches, or irregular activities involving maintained records.

14.3 Audit Trails

The License Holder shall maintain comprehensive and tamper-evident audit trails to ensure the accountability and traceability of all key system and user activities.

Audit trails shall be maintained for, at a minimum:

- Administrative and privileged user actions within the platform and systems;
- Financial adjustments, including manual corrections and operational interventions affecting player balances;

- Changes to account status, including account creation, suspension, limitation, or closure; and
- Security-related events, including access attempts, system alerts, and detected incidents.

All audit trail records shall:

- Be securely stored and protected against unauthorized modification or deletion;
- Include sufficient detail to reconstruct events and support investigations; and
- Be retained for a period consistent with regulatory, audit, and legal requirements.

The License Holder shall ensure that audit trails are regularly reviewed and are readily available for internal audits, external audits, and regulatory inspections.

15. AML/CFT COMPLIANCE

15.1 AML Framework

The License Holder shall establish, implement, and maintain a comprehensive Anti-Money Laundering and Counter-Terrorist Financing (“AML/CFT”) framework in accordance with applicable Curaçao legislation and relevant regulatory requirements.

The AML/CFT framework shall be designed to prevent, detect, and report money laundering, terrorist financing, and other forms of financial crime. It shall include documented policies, procedures, and internal controls governing customer due diligence, transaction monitoring, reporting obligations, and staff responsibilities. Responsibility for the effective implementation of the AML/CFT framework shall be assigned to a designated Money Laundering Reporting Officer (“MLRO”), who shall oversee compliance with all applicable obligations.

Further details are set out in the License Holder’s AML Policy, which forms an integral part of the overall compliance framework.

15.2 Risk-Based Approach

The License Holder shall apply a risk-based approach (“RBA”) to AML/CFT compliance, ensuring that customer due diligence and monitoring measures are proportionate to the level of risk identified.

Risk assessments shall take into account, at a minimum:

- Customer risk, including player profile, behavior, and source of funds;
- Geographic risk, including the jurisdictions in which players are located or operate;
- Transactional behavior, including volume, frequency, and patterns of deposits, withdrawals, and wagering activity; and
- Payment methods, including the type and risk profile of payment instruments used.

Enhanced due diligence measures shall be applied to higher-risk customers or transactions, while simplified measures may be applied in lower-risk scenarios, where permitted under applicable regulations.

15.3 Transaction Monitoring

The License Holder shall implement automated transaction monitoring systems to identify and assess potentially suspicious activity in real time and on a retrospective basis.

Monitoring systems shall be designed to detect, analyze, and flag:

- Unusual or inconsistent transaction patterns;
- Structuring or “smurfing” behavior aimed at avoiding reporting thresholds;
- Suspicious betting activity or irregular gameplay patterns; and
- Exposure to sanctioned individuals, entities, or jurisdictions.

Alerts generated by monitoring systems shall be reviewed promptly by qualified personnel, with appropriate escalation procedures applied where required.

15.4 Suspicious Transaction Reporting

Where suspicious activity is identified, the License Holder shall ensure that such matters are promptly escalated to the MLRO for assessment and determination.

Where required by applicable laws and regulations:

- Suspicious transactions shall be reported to the relevant competent authorities in a timely manner;
- Reports shall be submitted in accordance with prescribed formats and timelines; and
- Confidentiality shall be maintained to ensure that no unauthorized disclosure (including tipping-off) occurs.

The License Holder shall maintain records of all suspicious activity reports, including internal assessments and decisions, for audit and regulatory inspection purposes.

16. INCIDENT MANAGEMENT

16.1 Incident Categories

The License Holder shall identify, classify, and manage all incidents that may impact operations, system integrity, player protection, or regulatory compliance.

Incidents shall include, but are not limited to:

- Cybersecurity events, including unauthorized access, hacking attempts, or malware incidents;
- Fraud-related events, including payment fraud, bonus abuse, or collusion;
- Service interruptions impacting platform availability, transaction processing, or gameplay;
- Data breaches involving the loss, exposure, or compromise of personal or financial data; and

- Regulatory breaches, including failures to comply with Curaçao gaming legislation (LOK) or licensing conditions.

16.2 Purpose and Scope

The purpose of the incident management framework is to ensure that all incidents are:

- Identified, assessed, and classified without undue delay;
- Logged, tracked, and managed throughout their lifecycle in a consistent manner;
- Resolved efficiently to minimize operational, financial, and reputational impact; and
- Documented and analyzed to support continuous improvement and regulatory compliance.
-

This framework applies to:

- All operational, technical, and business incidents; and
- All internal personnel and third-party service providers involved in service delivery.

16.3 Incident Lifecycle Process

The License Holder shall ensure that all incidents are managed through a structured lifecycle process to ensure consistent handling, timely resolution, and full regulatory compliance.

Step 1: Identification

Incidents shall be identified through various detection mechanisms, including:

- Automated monitoring tools and system alerts;
- User or player reports; and
- Internal operational or security reviews.

All personnel and third-party providers shall promptly report any suspected or actual incidents upon detection.

Step 2: Categorization

Each incident shall be categorized according to its nature and origin, including but not limited to:

- Technical (e.g., network, application, infrastructure);
- Security (e.g., cybersecurity, data breach);
- Operational (e.g., service disruption); and
- Compliance-related (e.g., regulatory breach).

Appropriate categorization shall enable consistent reporting, analysis, and prioritization.

Step 3: Diagnosis

An initial assessment shall be conducted to:

- Determine the nature, scope, and impact of the incident;
- Identify affected systems, services, or users; and
- Apply initial troubleshooting steps using available documentation, including known error databases and resources.

Where possible, immediate corrective actions or workarounds shall be implemented.

Step 4: Escalation

Incidents shall be escalated as necessary, depending on their severity and potential impact:

- To relevant technical or operational teams for resolution;
- To senior management for material or high-risk incidents; and
- To the Compliance function where regulatory implications are identified.

Major incidents shall trigger enhanced response procedures, including:

- Appointment of an Incident Manager;
- Activation of coordinated response activities (e.g., incident bridge calls); and
- Increased communication and monitoring.
- Informing Managing Director

Step 5: Resolution

The responsible team shall:

- Investigate the root cause of the incident;
- Implement corrective actions or permanent fixes; and
- Ensure that any temporary workarounds are replaced with sustainable solutions.

All actions taken shall be documented, including:

- Resolution steps;
- Tools and system logs reviewed; and
- Technical or operational changes implemented.

Step 6: Recovery

Following resolution, the License Holder shall ensure full recovery of affected services by:

- Verifying system functionality and data integrity;
- Confirming that services have been restored to normal operational levels; and
- Monitoring systems for any residual issues or recurrence of the incident.

Step 7: Closure

An incident shall only be formally closed once:

- Resolution has been fully implemented and validated;
- Root cause analysis has been completed (where applicable);
- All required documentation has been finalized; and
- Relevant stakeholders or users have been informed, where appropriate.

Proper classification and tagging of the incident shall also be confirmed for reporting and audit purposes.

Step 8: Continuous Improvement

The License Holder shall conduct post-incident analysis to support continuous improvement, including:

- Reviewing incident trends and recurring issues;
- Identifying gaps in controls, processes, or systems; and
- Implementing corrective and preventive actions.

Findings shall be incorporated into:

- Problem Management processes;
- Change Management procedures; and
- Staff training and awareness programs.

16.4 LOK-Aligned Incident Reporting and Escalation Thresholds

The License Holder shall ensure that incidents are assessed against regulatory reporting thresholds and escalated accordingly.

16.4.1 Reportable Incidents

An incident shall be deemed reportable to the Curaçao Gaming Authority (CGA) where it involves, or is reasonably likely to involve:

- A material system failure affecting gaming operations, including outages or malfunction impacting fairness or availability;
- A cybersecurity incident compromising system integrity, availability, or confidentiality;
- A data breach involving unauthorized access, disclosure, or loss of personal or financial information;
- A failure affecting game fairness, including RNG issues, settlement errors, or incorrect payouts;
- Significant fraud or financial crime events, including large-scale fraud, AML/CFT concerns, or suspicious transaction patterns; and
- Any breach of regulatory obligations, license conditions, or player protection requirements.

16.4.2 Reporting Timelines

The License Holder shall ensure that reportable incidents are:

- Escalated internally without delay to senior management and the Compliance function;
- Reported to the CGA promptly, and in any event within regulatory timeframes applicable under LOK; and
- Followed by supplementary reporting, where required, providing updates on investigation outcomes, root cause, and remediation measures.

Where precise timelines are not explicitly defined, reporting shall occur as soon as reasonably practicable, taking into account the severity and impact of the incident.

16.4.3 Reporting Content Requirements

Reports submitted to the CGA shall include, at a minimum:

- A detailed description of the incident;
- Date and time of occurrence and detection;
- Systems, services, or players affected;
- Initial impact assessment (operational, financial, and regulatory);
- Immediate actions taken to contain the incident;
- Root cause analysis (where available); and
- Remediation and preventive measures implemented or planned.

16.4.4 Internal Escalation

All incidents shall follow structured escalation procedures, including:

1. Logging and classification within the incident management system;
2. Investigation and impact assessment;
3. Escalation to relevant technical, operational, and compliance teams;

4. Notification to senior management for material incidents; and
5. External reporting where required under regulatory obligations.

16.4.5 Documentation and Audit

The License Holder shall maintain complete and auditable records of all incidents, including:

- Incident logs and classifications;
- Investigation findings and supporting evidence;
- Communication records (internal and external); and
- Regulatory notifications and submissions.

All records shall be retained in accordance with applicable recordkeeping requirements and shall be made available to the CGA upon request.

16.5 Continuous Improvement

Incident data shall be analyzed on an ongoing basis to:

- Identify trends and recurring issues;
- Enhance controls, system resilience, and operational processes; and
- Inform updates to policies, procedures, and training programs.

17. APPENDICES

Appendix A – Infrastructure Diagram

Appendix B – overview Games of Chance, including a description of visual elements shown to players as part of the operation through the gaming website or other software application

Appendix C - Third-Party Provider overview

Appendix D – Overview payment methods

Appendix E – Technical measures for vulnerable player detection

Appendix F –Terms and Conditions

APPENDIX A – TECHNICAL INFRASTRUCTURE DIAGRAM

1. Core Platform Architecture

The License Holder operates an in-house developed online gaming platform consisting of the following core components:

- Web Application (Player Interface)
- Back Office Administration Portal
- Gaming Engine
- Wallet & Transaction Management System
- Player Account Management System
- Reporting & Analytics Module
- API Integration Layer

The platform operates in separate Development, Staging, and Production environments.

2. Hosting Environment

<u>Item</u>	<u>Details</u>
Hosting Provider	Hetzner Online GmbH
Infrastructure Type	Cloud Infrastructure
Production Environment	Hosted on dedicated cloud servers
Development Environment	Separate development environment
Data Centre Location	European Union

3. Critical Systems

<u>System</u>	<u>Description</u>	<u>Provider</u>	<u>Environment</u>
Gaming Platform	Core in-house online gaming platform	In-house	Production
Wallet System	Player wallet and balance management system	In-house	Production
Database	Player, transactional and gaming data storage	In-house (Hosted on Hetzner)	Production
Back Office System	Administrative and operational management platform	In-house	Production
Payment Gateway (Cards & E-wallets)	Card and e-wallet payment processing	Paysafe (Skrill & Neteller)	Production
Alternative Payments	Voucher-based payment processing	Flexepin	Production

<u>System</u>	<u>Description</u>	<u>Provider</u>	<u>Environment</u>
Banking Services	Corporate banking and settlement accounts	ISX Financial EU PLC	Production
Banking Services (Upcoming)	Additional banking integration	Bankera	Pending activation

4. Network & Security Architecture

The infrastructure includes:

- Network segmentation between environments.
- Firewall protection.
- Secure VPN access for authorized administrators.
- Role-Based Access Control (RBAC).
- Multi-Factor Authentication (MFA) for administrative accounts.
- Encryption of data in transit using TLS.
- Encryption of sensitive data at rest.
- Continuous monitoring of system availability and security events.

5. Third-Party Service Providers

<u>Service</u>	<u>Provider</u>	<u>Purpose</u>
Infrastructure Hosting	Hetzner Online GmbH	Cloud hosting for application, database and infrastructure services
Gaming Platform (Infrastructure Support)	In-house	Operation of core gaming platform and system architecture
Wallet & Back Office Systems	In-house	Player account management, wallet operations, and administrative system
Payment Gateway (Cards & E-wallets)	Paysafe (Skrill & Neteller)	Processing of card and e-wallet transactions
Alternative Payment Methods	Flexepin	Voucher-based deposit processing
Corporate Banking	ISX Financial EU PLC	Corporate banking and settlement services
Corporate Banking (Upcoming)	Bankera	Additional banking services (pending activation)
KYC / AML Verification	In-house	Customer identity verification and initial AML screening (engagement of an independent third-party provider is planned)

<u>Service</u>	<u>Provider</u>	<u>Purpose</u>
Monitoring & Security Tools	In-house / Standard infrastructure tools	System monitoring, uptime tracking, and operational security oversight

6. Backup & Disaster Recovery

- Daily automated backups of production databases.
- Regular backups of application files and configuration.
- Backup retention in accordance with the Company's Information Security Policy.
- Backup copies stored separately from production systems.
- Disaster Recovery procedures are documented and periodically reviewed.
- Recovery procedures are tested where appropriate to ensure operational resilience.

7. Infrastructure Change Management

Infrastructure changes are managed through the Company's Change Management procedures and include:

- Change request documentation.
- Technical review and approval.
- Testing prior to deployment.
- Controlled production release.
- Rollback procedures where applicable.
- Maintenance of change records.

8. Document Control

<u>Item</u>	<u>Details</u>
Document	Appendix A – Technical Infrastructure Diagram
Version	1.0
Effective Date	29.06.2026
Approved By	Director, eMoore N.V.
Review Frequency	Annually or upon material infrastructure changes

APPENDIX B – GAMES OF CHANCE REGISTER

Overview

The License Holder offers a portfolio of Games of Chance supplied by multiple licensed game providers through established gaming aggregators, as well as through direct integrations with selected licensed game providers where applicable.

The portfolio is continuously reviewed and may be updated by adding or removing games and providers in accordance with commercial requirements, technical integration, and applicable regulatory requirements.

Available Game Categories

<u>Category</u>	<u>Description</u>	<u>Source</u>	<u>Status</u>
Slots	Digital reel-based slot games	Licensed game providers via aggregators and direct integrations	Active
Roulette	RNG and Live Roulette games	Licensed game providers	Active
Blackjack	RNG and Live Blackjack games	Licensed game providers	Active
Baccarat	RNG and Live Baccarat games	Licensed game providers	Active
Live Casino	Live dealer games	Licensed game providers	Active
Sports Betting	Pre-match sports betting	Licensed sportsbook provider(s)	Active
In-Play Betting	Live sports betting	Licensed sportsbook provider(s)	Active
Virtual Sports	Virtual sporting events	Licensed providers	Active
Lottery Games	Lottery products	Licensed providers	Active
Instant Win Games	Scratch cards and instant win products	Licensed providers	Active
Bingo	Online bingo games	Licensed providers	Active
Keno	Number draw games	Licensed providers	Active
Crash Games	Multiplier-based games	Licensed providers	Active
Jackpot Games	Progressive and fixed jackpot games	Licensed providers	Active

Provider Management

The License Holder maintains commercial relationships with multiple licensed gaming aggregators and, where applicable, directly integrated licensed game providers. The list of providers and available game titles is maintained internally and updated on an ongoing basis as part of the Company's operational and supplier management procedures.

APPENDIX C - SOFTWARE PROVIDERS REGISTER

1. Overview

This Appendix provides an overview of the primary software providers and aggregation platforms engaged by the License Holder for the provision of gaming content. The Company utilizes a combination of direct integrations and third-party aggregators to deliver casino gaming content. All providers are subject to appropriate due diligence, contractual oversight, and ongoing compliance monitoring to ensure adherence to applicable regulatory, technical, and security standards.

2. Software Providers Table

Provider name	Type	Service/ Content Type	Licensing Jurisdiction	Certifications (RNG/ Testing)	Integration Type	Status
EAR	Aggregator	Casino Game Aggregation Platform	EU / B2B Gaming Jurisdiction	Certified via third-party suppliers	Aggregator	Active
Bromston Associates Ltd (SoftGamings)	Aggregator/ Platform	Gaming Platform & Aggregation Services	EU	ISO / RNG certified suppliers (where applicable)	Aggregator	Active
Hub88	Aggregator	Casino Game Aggregation Platform	Malta / EU	GLI / iTech Labs certified suppliers (where applicable)	Aggregator	Active
EGT	Game Provider	Slot Games	Bulgaria / EU	GLI certified RNG	Direct + Aggregator	Active

Endorphina	Game Provider	Slot Games	Malta / EU	GLI / iTech Labs certified RNG	Direct + Aggregator	Active
Ezugi	Live Casino Provider	Live Dealer Games	Malta / EU	eCOGRA / GLI certified systems	Direct + Aggregator	Active
Lucky Streak	Live Casino Provider	Live Dealer Games	Malta / EU	GLI certified systems	Direct + Aggregator	Active
Playson	Game Provider	Slot Games	Malta / EU	iTech Labs / GLI certified RNG	Direct + Aggregator	Active

3. Aggregation Model Statement

The License Holder operates a hybrid integration model consisting of both direct integrations with selected game providers and indirect access via approved aggregation platforms.

Aggregators are responsible for onboarding, certification verification, and ongoing compliance monitoring of underlying third-party game providers. The License Holder ensures that all aggregated content originates from properly licensed and certified sources.

4. Due Diligence & Compliance

Prior to integration, all software providers are subject to due diligence procedures including verification of licensing status, technical certification, and regulatory standing.

Providers are continuously monitored to ensure ongoing compliance with applicable technical standards, including RNG integrity, game fairness, cybersecurity, and operational resilience requirements.

5. Change Management & Technical Control

All software updates, modifications, and integrations are subject to formal change management procedures, including testing, approval, and controlled deployment.

Any changes affecting game logic, functionality, or system performance are reviewed prior to production release.

6. Record Keeping & Auditability

The License Holder maintains comprehensive records relating to all software providers, including contracts, certifications, integration logs, and version history.

All records are stored in a secure and structured manner and are available for inspection by relevant regulatory authorities upon request.

7. Internal Register Reference

A full and detailed register of all software providers, including downstream providers accessed via aggregation platforms, is maintained as a controlled internal document and may be made available to the relevant regulatory authority upon request.

APPENDIX D – PAYMENT METHODS AND PROVIDERS REGISTER

1. Overview

The License Holder supports a range of payment methods for deposits and withdrawals, facilitated exclusively through regulated and reputable Payment Service Providers (PSPs), voucher-based payment solutions, and licensed banking institutions.

All payment transactions are processed in accordance with applicable regulatory requirements, AML/CTF obligations, and internal financial controls. The License Holder does not store or process sensitive payment card data.

2. Accepted Payment Methods and Providers

<u>Payment Method</u>	<u>Provider</u>	<u>Purpose</u>	<u>Status</u>
Credit / Debit Cards	Paysafe	Deposits and withdrawals (where supported)	Active
E-Wallets (Skrill)	Paysafe (Skrill)	Deposits and withdrawals	Active
E-Wallets (Neteller)	Paysafe (Neteller)	Deposits and withdrawals	Active
Voucher Payments	Flexepin	Prepaid voucher-based deposits	Active
Bank Transfers	ISX Financial EU PLC	Deposits and withdrawals	Active
BankTransfers (Upcoming)	Bankera	Deposits and withdrawals	Pending activation

3. Payment Processing Framework

All payment transactions are processed exclusively through licensed third-party Payment Service Providers, voucher-based systems, or regulated banking institutions.

The License Holder does not directly process, store, or transmit sensitive cardholder data. All card and e-wallet transactions are handled within the secure environments of the respective Payment Service Providers.

Payment processing includes:

- Secure redirection to PSP or banking environments
- PCI-DSS compliant processing via PSP infrastructure
- Transaction validation and monitoring for fraud prevention
- AML screening and risk-based transaction monitoring

4. Banking Infrastructure

The License Holder maintains operational banking relationships with regulated financial institutions to support fiat transactions and corporate financial operations:

- **Current banking provider:** ISX Financial EU PLC
- **Upcoming banking provider:** Bankera (integration pending activation)

All banking partners are selected based on regulatory compliance, operational reliability, and support for cross-border payment processing activities.

5. Financial Controls

The License Holder applies the following financial safeguards:

- Segregation of player funds from operational company accounts
- Transaction monitoring for fraud detection and AML compliance
- Deposit and withdrawal limits based on risk scoring and verification level
- Withdrawal approval procedures subject to KYC verification status
- Continuous review of payment provider performance and compliance status

6. Payment Method Expansion

The License Holder may, from time to time, introduce additional payment methods and providers, and continuously reviews its payment infrastructure to ensure alignment with regulatory requirements, risk management policies, and business needs.

7. Document Control

Version: 1.0

Date: 29.06.2026

Approved By: Director, eMoore N.V.

Review Cycle: Annual or upon material changes in payment infrastructure

APPENDIX E - VULNERABLE PLAYER DETECTION – TECHNICAL AND OPERATIONAL CONTROLS

1. Overview

This Appendix describes the technical and operational controls implemented by the License Holder to identify, monitor, and respond to indicators of potentially vulnerable or at-risk gambling behaviour. These controls form part of the Company's Responsible Gaming framework and are designed to support early detection and appropriate intervention in accordance with internal policies and applicable regulatory requirements.

2. Automated Monitoring System

The gaming platform operates a rules-based automated monitoring system that continuously analyses player activity to identify behavioural patterns potentially associated with gambling-related harm.

The monitoring system evaluates, without limitation, the following indicators:

- Deposit frequency and transaction values;
- Significant increases in deposit amounts over time;
- Rapid, continuous, or repetitive wagering behaviour;
- Extended or uninterrupted gaming sessions;
- Short session intervals indicating persistent play behaviour;
- Multiple failed deposit attempts or irregular payment patterns;
- Abnormal withdrawal or cancellation activity (where applicable);
- Sudden deviations from established player behaviour patterns;
- High loss frequency within short timeframes.

The system generates automated alerts when predefined risk thresholds or behavioural triggers are met or exceeded.

3. Risk Assessment and Classification

Alerted player activity is subject to internal assessment and may be classified according to risk level, including:

- Low Risk
- Medium Risk
- High Risk

Risk classification is based on the severity, frequency, and combination of detected behavioural indicators and determines the level of review and intervention required.

4. Manual Review Process

All alerts classified as medium or high risk are reviewed by authorized Responsible Gaming and/or Compliance personnel.

The review process may include:

- Analysis of transaction and betting history;
- Evaluation of gameplay behaviour and session data;
- Review of account verification (KYC) status;
- Assessment of previous Responsible Gaming interactions;
- Consideration of any direct player communications.

Where necessary, the Company may request additional information or clarification from the player to support the assessment.

5. Responsible Gaming Interventions

Based on the outcome of the review, the Company may apply one or more of the following measures:

- Responsible Gaming notifications or warnings;
- Direct communication with the player;
- Deposit limits;
- Loss limits;
- Wagering limits;
- Session time reminders or reality checks;
- Cooling-off periods;
- Temporary account restrictions;
- Self-exclusion measures;
- Permanent account closure, where deemed necessary.

6. Ongoing Monitoring

Player activity is subject to continuous monitoring throughout the entire customer lifecycle.

Risk assessments are updated dynamically upon detection of:

- Material changes in gambling behaviour;
- Significant changes in deposit or wagering patterns;
- New automated alerts;
- Responsible Gaming interactions or player requests.

7. Record Keeping

All alerts, reviews, risk assessments, and Responsible Gaming actions are recorded and securely maintained within the Company's internal systems.

Records are retained in accordance with internal compliance procedures and applicable regulatory obligations.

8. Related Policies and Procedures

This Appendix should be read in conjunction with the following internal documents:

- Responsible Gaming Policy
- AML/CFT Policy
- Customer Due Diligence Procedures
- Operational Manual

APPENDIX F –TERMS AND CONDITIONS

TERMS AND CONDITIONS Last update: 24 July 2025

1. All the bets made with reference to the services rendered by our company are subject to regulations, which can be modified, when necessary and during the internet site's operation term, after our clients have first been informed via our internet site address.

2. An individual cannot make use of the Services unless that individual is over eighteen (18) years of age or any legal age at which gambling or gaming activities are permitted under the law or jurisdiction applicable to his person and has successfully registered for a Player Account. If

company detects that a minor has created an account, the company has the right to void any winnings and close the account.

3. Each client is responsible to keep his account password private. Any bets made in his/ her account by any third party that knows his/ her password will be considered valid.

4. Each person can open only one account in Goalbet. The company has the right to close down the accounts of any client who has opened a number of accounts in his/ her name, or in different names, in order to deceive the company. Goalbet has also the right to cancel any transaction associated with an attempt to deceive the company. In such cases it is at the sole discretion of the company to put all the tickets equal to the unit and to return the money, after deducting the expenses.

5. Goalbet has the right to deny the creation of a new betting account.

6. The application for the opening of an account is submitted by filling-in the Registration form and sending it to Goalbet. Kindly bear in mind that the money in your betting accounts neither include nor can claim interests.

7. The minimum deposit per account is 1 Euro, or any equivalent amount in any other currency.

8. Any suspicion related to the eventually illegitimate carrying out of a game, or a sport venue may lead Goalbet to withdraw the payments until the case has been fully investigated. Any such investigation will be carried out in cooperation with the competent State, or Independent Authorities. Any bets made for such venues may be declared void and the wagers may be returned.

9. The results of the sport venues are the ones stated upon their ratification by the official competent organs, unless it is otherwise specified. Any change of the result, after the ratification, shall have absolutely no impact on the betting.

10. Goalbet has the right to deny for any user, in whole or in part, any betting.

11. A betting slip sent for confirmation shall be considered valid only after it has been confirmed and only for the amount of money that it has been confirmed.

12. All the clients shall always ensure: - That they fill-in their true residence address - That they register in their own name - That they fill-in their true e-mail address - That they fill-in their true residence telephone and cell phone numbers - That they hold one and only one betting account - That they do not act for somebody else's interest, or on somebody else's account - That they do not deposit money that comes from criminal activities - That they do not use their account for money 'laundering'.

13. The placement of multiple bets for a single event is impossible. Should such thing happen, due to a human, or a system-related mistake, all the bets placed for such event will be cancelled. In such case, the odds will be equal to 'one' (1).

14. No confirmed bet can be modified, or cancelled, by the player. The company has the right to cancel accepted bets before the beginning of the game, without justification, only upon notification of the client, by an e-mail sent to the address he/ she stated in the registration form, or by contacting him/ her by telephone.

15. In case the date, or the hour of a venue is postponed, the slips that were submitted before the initial date and hour of the venue will be considered valid. The bets that were submitted after the

initial date and hour of the venue will be considered void. If the game is included in a slip, together with other games, this particular game will be given 'one' (1).

16. The odds of the venues may present variations during the venues. The applying odds will be those indicated on the slip, upon the acceptance of the bet.

17. In case of a visible mistake in the published odds, the company has the right to correct the faulty odds, and to simultaneously cancel the slips containing this particular game, even if the result of the game has already been shaped. In case of a single result, the wager is returned to the player. In case of multiple bets, the game will be given 'one' (1).

18. Each customer is under a specific license and may not be connected to a VPN changing the use of the license that was issued when he opened his account. If a customer changes the license and the country which he belongs to using VPN, the company is required for tax and legal reasons to set all the coupons that have been played since he used the VPN equal to the unit and to return the money in the client's account to the corresponding license that has made the deposit.

19. The minimum bet is 50 cents of a Euro, or any equivalent amount in any other currency.

20. The maximum profit is five thousand times the betting wager.

21. The maximum total profit for multiple betting, using similar venue combinations and/or same match, for single bets is limited to the amount of 5,000€ (Euro), for multiple or system bets is limited to the amount of 15,000€ (Euro). Each customer can request VIP limits, with which the maximum profit per bet, for single bets or multiple and system bets, is unlimited.

22. All the profits will be credited in the Goalbet client's betting account.

23. The profits will be paid regularly, in the account's currency.

24. If a game is interrupted or postponed and not finished in a period of 24 hours, the bet will be considered void and the odds will be equal to 'one' (1) for all betting options. The bets that have been completed before the interruption of the game will be considered active.

25. Any game postponed (Football, Basketball, Tennis, Handball, Formula 1, Motorcycles) for more than 24 hours will be considered void, if it is not finished or not replayed. The odds will be equal to 'one' (1).

26. The dates, home teams and times displayed for every match are for reference only. The actual game date, time and court for every match is determined from the official game regulator. In case of date misplacement of a match (from Goalbet), then all bets which were accepted before the official match start will be considered valid, while all bets which were placed after the official match start or with wrong home team, will be considered void and the odd shall be equal to 1.00.

27. Any bet that has not been confirmed before the first game will be considered void. A bet will be considered won if it appears on the betting list of the user's account.

28. Goalbet is in no case responsible for problems related to problematic PCs, telecommunication lines or internet connections, nor for play methods implemented by clients who are not approved by our company.

29. In spite of the fact that all the necessary measures are taken, in order to protect the Software against viruses, we cannot and will not guarantee you that your PC will not be affected, with such thing resulting to the interruption of our services. The services will be rendered again, within the

reasonable time period required for the restoration of any damage you may suffer, after the interruption of our services.

30. By accessing the Internet Site Addresses of Goalbet you accept the terms and requirements of this agreement. If you do not agree with the above terms and requirements, please, do not access our internet site addresses.

31. As a requirement for the use of the Internet Site Addresses of Goalbet, one must guarantee that the internet site addresses will not be used for illegal purposes, or purposes violating the above terms and requirements.

32. If any part of this agreement becomes void, or does not conform to the applying laws, including, without limitation, the guarantees and the liabilities stipulated above, an applying term, matching the intentions of the initial purpose will prevail over such void or non-conforming part of the agreement, while the rest of the agreement will remain in force.

33. The Terms and conditions apply to all types of betting, unless differently stated to the individual explanatory categorization field.

34. On the provision of any rights not included hereto.

35. This agreement is subject to the Laws of Curacao

36. The accounts of players using Sure Bet, Value Bet, Trading. will be deactivated upon decision of the relevant department and any profit that has been arisen from the use of these methods is deducted from the customer's balance. Furthermore, the customer is responsible for any bank transfer fees that may arise during the process of processing the relevant withdrawal request.

37. User is obligated to upload the necessary files in order to verify the account and use our services.

38. User is being checked by the Hampi Check system in order to prohibit the use of our services in case there is an active ban rule for the account.

39. By accepting the terms and conditions of our company, the user accepts that our company has the right to conduct any identification and verification checks, which deems necessary and request the user to send further identification and verification documents. The user also agrees to provide all the information that will be required for the authentication check. During and until the identification checks are completed, our company reserves the right to suspend or restrict the user's account.

40. DIGIBET N.V. is making a great effort to safeguard the rights of its employees and to provide them with a more enjoyable working environment as possible. For this reason, if there is a violent, indecent or/and offensive attitude of a client towards our employees, the Company reserves the right to suspend or/and disable a user's account.

41. You are not allowed to register a new account or place any bet or wager through this website if you are located in the Jurisdiction of Essen, at the time of registration or the playing of any games.

42. In case of free bet wager, the FreeBet amount is deducted from the total winnings.

DEPOSIT/ WITHDRAWAL/ REFUNDS/ MONEY LAUDERING

Goalbet has the right to cancel or declare as void (in its sole discretion) transactions of what kind so ever that show irregularities, in particular irregularities of the following nature:

- 1) The name and address of the player do not match the name and address associated with the credit card, or other mode of payment, used by the player/customer.
- 2) Any irregularity which may negatively affect the processing of payment transactions and/or which gives rise to the suspicion of a violation of the General Terms and Conditions.
- 3) Goalbet takes any form of fraudulent activity of players/customer in connection with services and/or products offered by Goalbet very seriously. Any fraudulent activity, as determined at Goalbet's sole discretion, is strictly prohibited. Fraudulent activity may include, but is not limited to, stolen credit cards, transfer of funds to other player accounts (chip dumping), forgery, collusion, the provision of false registration data or other requested information. In addition to any other remedies provided under the general terms and conditions or the applicable game rules, Goalbet reserves the right to pursue claims for criminal prosecution and/or civil damages for any fraudulent activities. For this purpose, Goalbet furthermore reserves the right to record telephone calls with customers in order to pass on to third parties for the purpose of prosecution. Any player/customer involved in any form of suspected fraudulent activity and any suspicious transaction will be reported to the appropriate authorities.
- 4) Furthermore, it is strictly prohibited to deposit funds derived from illicit or unlawful activities into the Goalbet Account. The Company conducts thorough monitoring and verification of all transactions in order to prevent money laundering and the financing of terrorist activities. Suspicious transactions will be reported to the authorities in charge.
- 5) Where deposits/withdrawals are made by electronic payment methods (eg electronic wallet), the customer is required to use his personal electronic payment account. In the event that third-party electronic payment accounts are used, then all winnings made after the deposit with this electronic payment account are canceled and the deposits are refunded to the third-party electronic payment account after deducting any costs. Our company also reserves the right to deactivate the client's account if there is an infringement of this rule.

Any decision of Goalbet regarding the invalidation of transactions shall be binding upon the player/customer and lies within the sole discretion of Goalbet and may not be contested by the player/customer. In case of any irregularities in payment transactions as described in 1) to 4) above or in case of reasonable suspicions concerning the violation of any rules governing gaming or betting at Goalbet (i.e. these General Terms and Conditions, the rules of the game and specific rules as applicable) Goalbet may at its sole discretion, declare the transactions concerned invalid.

In every case Goalbet reserves the right to hold/charge costs which can occur after each procedure (transaction fees, court costs etc.).

Deposits made to your goalbet account should be played three (3) times in odds 1.80 (per event) and more before you can request a withdrawal (e.g. If you deposit 10 EUR, your total betting cost should be at least 30 EUR in odds 1.80 (per event) and more in order to request withdrawal). The bets with odds less than 1,80 (per event) will not count for the deposit rollover. (The bet/bet slip that contains selections of Draw No Bet/Asian Handicap / Cashout and Postponed matches do not count for deposit rollover). Therefore, if in goalbet's discretion, there is suspicion of abuse (for instance, where a deposited amount has not been used for an appropriate level of game play and the user then makes a withdrawal request in relation to that deposited amount), goalbet reserves the right in its absolute discretion to cancel the respective deposit(s) in part or in full, to retract any costs that may have resulted in conjunction therewith and to close the goalbet account indefinitely. Goalbet further reserves the right to request and obtain satisfactory proof of deposit and additional copies of personal identification in such instances prior to processing any withdrawal request, the processing of such request to be entirely at Goalbet's discretion.

PROHIBITED JURISDICTIONS RULE

Players residing in the following countries are prohibited to register an account: Curacao, the Netherlands (and any country forming part of the Kingdom of the Netherlands), the United States and FATF blacklisted countries (North Korea, Iran, Myanmar) France, Australia, Spain, Belgium, Switzerland, Poland, Lebanon, Cyprus, Singapore, Qatar, Japan, Cambodia, Brunei, United Arab Emirates, Russia, Iraq, Afghanistan, UK, USA, Azerbaijan, Armenia, Lithuania, Ukraine, Russia, Croatian, Kazakhstan, Kyrgyzstan, Moldova, Denmark, Serbia, Slovakia, Uzbekistan, Turkey.

The operation of our company in the above countries is prohibited as these countries require a national license or generally ban gambling or are considered as prohibited areas by the international authorities and our company. In the event that a customer is found who plays either betting or casino in any of the above countries - while this is prohibited according to the rules accepted during registration - then our company reserves the right to return the deposit amount to the customer, to deduct any profits from him and to permanently deactivate his account.

Furthermore, the entities sanctioned by U.N., OFAC and EU where the client registers from that country, an EDD must be performed. EDD is performed on players from the following countries: Venezuela, Somalia, Afghanistan, Belarus, Congo, Nicaragua, Cuba, Eritrea, Iran, Somalia, Palestine, Myanmar, Sudan, South Sudan, Russia, Ukraine, Libya, Haiti, Yemen, Bosnia and Herzegovina, Zimbabwe, Mali, Niger.

6) Eligibility Refunds are available to Clients who deposited funds in their Trading Account(s) but has not open any transaction yet. In such case a client may be refunded regardless whether or not he/she has provided the Company (Digibet N.V.) with all the necessary Verification Documents.

6.1) Procedure

A) Eligible Client shall contact the Company (contact details are provided on the Company's Website) and request the initiation of the refund procedure in writing via email. The Client shall use only his/her registered e-mail address when requesting a refund.

B) Client's funds shall be returned to the same source, via the same payment method and remitter used to conduct the initial deposit, however if for whatever reason, the Company (Digibet N.V.) will not be able to proceed with such payment, the Company reserve the right to transmit the funds via an alternative payment method approved, verified and/or suggested by the Company (Digibet N.V.), at its sole discretion.

C) The Client who is eligible for a refund is not required to provide the Company with Verification Documents. However, certain payment providers may not provide the Company with all the necessary information regarding the origin of funds and, in such cases, and in accordance with the applicable regulatory framework (21/42 CIF 182/12 Privacy Policy Terms and Conditions of Use), the Company (Digibet N.V.) shall be entitled to request a bank transfer confirmation from the Client in order to duly proceed with the refund.

D) The Client understands and agrees that certain payment providers do not provide the Company (Digibet N.V.) with all the necessary information regarding the origin of funds and in such cases, in order to proceed with the refund, the Company shall request additional documents from the Client (i.e. Proof of Deposit in the form of a bank transfer confirmation, which will indicate the details of the bank account used for the initial deposit)

6.2) Time Restrains Upon receiving a request from the Client, the Company (Digibet N.V.) shall proceed with the payment of a specified amount within the same day or depending on the time the refund request has been received the latest the next working day (however, the time needed for the funds to reach the Client may vary, depending on Client's selected payment method). However, if the source of funds is not clear to the Company, the Company shall request additional documents for the Client, which may significantly delay the refund process.

7) Complaints

The Company will engage an independent Alternative Dispute Resolution (ADR) entity approved by the Curaçao Gaming Authority to provide an ADR procedure. This procedure will become effective once the Curaçao Gaming Authority publishes the list of certified ADR providers and the relevant guidelines.

The Player can submit a complaint within six months after the incident or bet settlement.

The Player cannot sell, donate, rent out, lease, pawn or pledge, under any title, any of their claims against the Company.

If the Player has any complaints on the performance of the Company under the agreement governed by the Terms, the Player should address the complaint to the Customer Support Team. If the initial response of the Customer Support Team is unsatisfactorily, the Customer may find the player complaint submission form via their account or request one via the Customer Support Team and submit this accordingly. An example of the player complaint submission form can also be found on the website of the Company, but as it is important to be able to verify that the complaint originates from a registered Player, the Form can only be submitted via the abovementioned mediums, including email. Upon receiving the player complaint submission form via one of these mediums, it becomes a Reportable Complaint in case the identification of the Customer can be verified.

On the Complaint Submission Form the following details needs to be provided:

- A. Customer's name, address and place of residence;
- B. Customer's account number or name;
- C. Date of the complaint and date of the disputed event;
- D. Description of the conduct being disputed;
- E. Amount in dispute.
- F. URL

Depending on the nature of the complaint, the Customer Support Team shall acknowledge the complaint within 2 business days (in case of responsible gaming complaint) or 1 week (for other complaints).

The aim of the Company is to solve complaints regarding Responsible Gaming within five (5) working days. In case more time is needed to make a reasonable and informed decision, this period can be extended with two (2) weeks. Players will be informed about this delay. If a delay is due to a lack of or slow response from the Player, the resolution period may be extended by another two (2) more weeks.

The aim of the Company is to solve all other types of complaints within four (4) weeks, which can be extended with another 4 weeks in case of complexity of the complaint or slow response by the player. The extension will be communicated accordingly to the Player. If the Complaint is not wholly resolved after the abovementioned conversations, the Player may address ADR, free of charge. The Company will bear all costs of the ADR process. Unless otherwise agreed, the ADR process will start not later than four (4) weeks after the date of the ADR Notice.

A decision of an ADR entity is binding both upon the Company, as well as the Player who referred the Reportable Complaint. The Player can only bring complaints to ADR if:

- the value of the complaint is more than EUR 5.000, - or
- if the Complaint pertains to a Responsible Gaming Complaint.

The Player may not commence any court proceedings/arbitration in relation to the dispute until it has attempted to settle the Complaint by arbitration and either the arbitration has terminated, or the Company has failed to participate in the mediation, provided that the right to issue proceedings is not prejudiced by a delay.

It is noted by Parties that the Curacao Gaming Authority (CGA) will not resolve or make decisions on any Player Complaints nor will act as an ADR/escalation entity as it does not mediate in individual disputes. CGA can be contacted by the Player with regards of matters such as malpractice, breach of license conditions or whistle blowing.