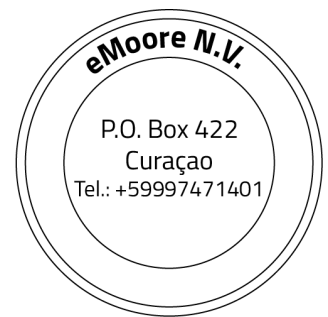


OPERATIONAL MANUAL

GMFY TECH N.V.

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 GMFY Tech N.V. (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

Legal Name: **GMFY Tech N.V.**

Commercial Name: **GMFY Tech N.V.**

Registration Number Chamber of Commerce: **148776**

Registered Address: **Groot Kwartierweg 10, Livestrong Building, Curacao**

Website(s)/URL(s): <https://casinoglory.com/> (not live yet)

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:

***Note:** as the Company is not live yet, the Company expects to offer all games of chance mentioned below, but that this operational manual shall be amended once the Company is indeed live, as some of the operational elements need to be defined and reviewed further upon commencement of the actual operations.*

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.

Additional Gambling Products

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 win.

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

Disaster Recovery Testing

Access Control Reviews

System Availability Monitoring

Transaction Monitoring

Responsible Gaming Monitoring

Minimum Frequency

Monthly and after major changes

At least annually or after significant changes

Quarterly

Annually

Quarterly

Continuous (24/7)

Continuous

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

A copy of these notices is included in **Appendix E**.

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 F** 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

[INSERT CURRENT NETWORK AND INFRASTRUCTURE DIAGRAM]

The diagram shall include:

- Hosting architecture
- Data flows
- Security layers
- Payment gateway integrations
- Backup infrastructure
- Redundancy architecture
-

10.3 Business Continuity Plan (BCP)

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

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

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 G.**

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 COMPLIANCE15.1 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

GMFY TECH N.V.

<https://casinoglory.com>

INFRASTRUCTURE DESCRIPTION

SECTION 1
OVERVIEW & PURPOSE

This document provides a structured description of the technical infrastructure supporting <https://casinoglory.com>, operated by GMFY Tech N.V. under the Curaçao gaming licence (LOK).

Area Covered	Description
Hosting Architecture	Physical datacenter, compute hosts, network, and application stack
Data Flows	How player traffic, game data, and transactions flow through systems
Security Layers	Perimeter, network, host, application, and data security controls
Payment Gateway Integration	How payment processing connects to the platform
Backup Infrastructure	Three-tier backup strategy: Veeam, PowerStore, Amazon S3 Glacier
Redundancy Architecture	Redundancy at network, compute, storage, and CDN layers

SECTION 2

HOSTING ARCHITECTURE

Casino Glory operates from a single Active Site hosted at the Primetel Nicosia Datacenter in Cyprus. All production compute, networking, and storage is located within this facility. Player-facing internet traffic is routed through Cloudflare before reaching the datacenter. Long-term backup data is replicated offsite to Amazon S3 Glacier.

2.1 Active Site — Primetel Nicosia Datacenter

Active Site: Primetel Nicosia Datacenter, Cyprus. Public IP Range: 109.105.254.201/29. This is the sole production hosting environment for all <https://casinoglory.com> services.

2.1.1 Internet & CDN Layer

Component	Provider / Model	Function
Public IP Range	Primetel ISP	Internet ingress and egress for all traffic
CDN / DDoS / WAF	Cloudflare	All inbound player traffic passes through Cloudflare: CDN caching, DDoS mitigation, WAF, SSL/TLS termination

2.1.2 Perimeter Firewall

Component	Type	IP Addresses	Function
pfSense Firewall	pfSense virtual machine (running on VMware ESXi)	External/ Internal	Stateful packet inspection, NAT, traffic filtering, and routing between the Primetel ISP uplink and the internal datacenter LAN

The pfSense firewall is deployed as a virtual machine on the VMware ESXi cluster, meaning its availability is dependent on the underlying ESXi host and PowerStore storage being operational. See Section 7 for redundancy notes.

2.1.3 Core Network Layer

Component	Model	Cluster IP	Configuration
Core Switch 1	Cisco Switch	10.122.120.200	Redundant switch cluster — Switch 1 of 2
Core Switch 2	Cisco Switch	10.122.120.200	Redundant switch cluster — Switch 2 of 2
LAN Segment A	[Compute VLAN]	10.122.104.131	Internal compute/application network segment
LAN Segment B	[Data VLAN]	10.122.120.120	Internal data and storage network segment

Each of the four physical ESXi servers has one physical connection to each switch in the Cisco switch cluster, providing link-level redundancy at the compute layer.

2.1.4 Compute Layer — VMware ESXi Virtualisation

All production virtual machines run on a four-node VMware ESXi cluster hosted on DELL PowerEdge R7625 servers. This cluster provides the compute foundation for all platform services.

Host	Hardware	Management IP	Status
ESXi 1	DELL PowerEdge R7625	10.122.120.121	Production virtualisation host
ESXi 2	DELL PowerEdge R7625	10.122.120.122	Production virtualisation host
ESXi 3	DELL PowerEdge R7625	10.122.120.123	Production virtualisation host
ESXi 4	DELL PowerEdge R7625	10.122.120.124	Production virtualisation host

2.1.5 Application Layer — Virtual Machines

The following application services are deployed as virtual machines across the ESXi cluster:

VM / Service	Type	Function
pfSense Firewall VM	Firewall (virtual)	Perimeter firewall and NAT router — external: / internal:
web-panel-1	Web Server / API	Front-end web server and API endpoint serving casinoglory.com (1 of 3)
web-panel-2	Web Server / API	Front-end web server and API endpoint serving casinoglory.com (2 of 3)
web-panel-3	Web Server / API	Front-end web server and API endpoint serving casinoglory.com (3 of 3)

VM / Service	Type	Function
Gaming Platform	Core Application	Casino Glory gaming engine, bonus engine, risk engine, RNG interface, and administrative backend
REDIS Production Cluster	In-memory Data Store	Session management, player state caching, and real-time game data; part of the STATIC ASSETS / REDIS Production Cluster
Static Assets Service	Content Delivery	Serves static game assets; part of the STATIC ASSETS / REDIS Production Cluster

2.1.6 Storage Layer

Component	Model	IP / Location	Function
Primary SAN Storage	DELL PowerStore 1200T	Primetel DC	Primary SAN storage for all ESXi VM datastores, databases, and application data
Backup Appliance	DELL DataDomain (PowerVault)	On-site (Primetel DC)	Veeam backup target; deduplication appliance storing compressed VM backup images

SECTION 3

DATA FLOWS

This section describes the primary data flows through the Casino Glory infrastructure, from player browser to backend systems and external providers.

3.1 Player Traffic Flow (Inbound)

All player internet traffic is routed through Cloudflare before reaching the Primetel datacenter. Cloudflare acts as the single point of internet ingress, providing DDoS mitigation, WAF filtering, and SSL termination.

1

Player Browser → Cloudflare

Player navigates to casinoglory.com. DNS resolves to Cloudflare's anycast IP. Cloudflare handles SSL/TLS termination and applies WAF rules and DDoS mitigation before forwarding.

2

Cloudflare → Primetel ISP Uplink

Clean (filtered) traffic is forwarded by Cloudflare to the Primetel public IP range. This is the datacenter's internet-facing ingress point.

3

Primetel Uplink → pfSense Firewall VM

Traffic hits the pfSense firewall virtual machine. pfSense performs stateful packet inspection, applies firewall rules, and performs NAT before forwarding to the internal LAN.

4

pfSense → Cisco Switch Cluster

Traffic enters the internal LAN via the Cisco switch cluster. The dual-switch configuration provides redundant path distribution to all compute hosts.

5

Cisco Switches → Web Panel VMs (web-panel-1/2/3)

HTTP/HTTPS requests are distributed across the three web-panel API servers. The web panels handle player authentication, session management, and API requests.

6

Web Panels → Gaming Platform VM + REDIS Cluster

Game logic requests are forwarded to the Gaming Platform VM. Player session state and cached data are read from and written to the REDIS Production Cluster.

7

Gaming Platform → DELL PowerStore 1200T

Persistent data (player accounts, wallet balances, transaction records, game logs, audit trails) is read from and written to the primary storage on DELL PowerStore 1200T .

3.2 Game Data & Outcome Flow

1

Player Places Wager

Wager submitted via web-panel API. Gaming Platform validates bet against game configuration and player account limits.

2

RNG / Game Logic Determines Outcome

For casino games: the certified RNG system (running within the Gaming Platform VM) generates a cryptographically secure random outcome. For third-party games: outcome is determined by the external game provider's certified RNG API and returned via the integration.

3

Settlement & Wallet Update

The gaming platform applies the outcome, updates the player wallet balance in the PowerStore database, and writes a tamper-evident game round log entry to the audit trail.

4

Result Returned to Player

Game result is returned via the web-panel API through Cloudflare to the player's browser in real time. REDIS cache is updated with the player's current session state.

3.3 Backup & Replication Data Flow

1

VM Data → Veeam Backup → DELL DataDomain

Veeam Backup & Replication continuously or periodically captures VM image backups from the ESXi cluster. Backup jobs write compressed and deduplicated backup images to the DELL DataDomain (PowerVault) appliance on-site within Primetel.

2

PowerStore Hourly Snapshots

DELL PowerStore 1200T generates hourly storage-level snapshots of all production volumes, providing rapid point-in-time recovery capability with an RPO of ≤ 1 hour without requiring a full Veeam restore.

3

DataDomain / Backup Data → Amazon S3 Glacier

Backup data is replicated from the on-site backup infrastructure (DataDomain / Veeam) to Amazon S3 Glacier for long-term offsite cold storage. This provides geographic separation from the Primetel Nicosia Datacenter.

3.4 Administrative & Monitoring Data Flow

- Administrative access to ESXi hosts, pfSense, PowerStore, and application backends is via secured management interfaces within the Primetel LAN, protected by RBAC and MFA.
- All administrative actions are logged to an immutable audit trail per the License Holder's audit trail requirements.
- 24/7 monitoring systems collect metrics from all infrastructure components and generate alerts for on-call personnel.
- AML/CFT transaction monitoring runs continuously against all financial data flows, with alerts escalated to the MLRO as required.

SECTION 4

SECURITY LAYERS

The Casino Glory infrastructure implements a defence-in-depth security model with distinct security controls at each architectural layer. The overall security framework is ISO 27001-aligned and complies with Curaçao gaming legislation (LOK) requirements for system integrity, data protection, and access control.

4.1 Security Architecture Overview

Layer	Location	Primary Control	Mechanism
L1 — Internet Edge	Cloudflare (external)	DDoS mitigation + WAF	All traffic filtered by Cloudflare before reaching the datacenter
L2 — Perimeter	pfSense VM (Primetel)	Stateful firewall + NAT	pfSense inspects and filters all traffic entering/leaving the internal LAN
L3 — Network	Cisco Switch Cluster	VLAN segmentation + ACLs	Internal network segmented into compute and data VLANs; switch ACLs applied
L4 — Host	VMware ESXi (x4 hosts)	Hypervisor isolation	VM isolation enforced at hypervisor level; each VM operates in isolated context
L5 — Application	Web Panels + Gaming VM	Authentication + RBAC	MFA on all admin access; RBAC controls player and staff access
L6 — Data	DELL PowerStore 1200T	Encryption at rest + at transit	All data encrypted in transit (TLS) and at rest (storage encryption)

Layer	Location	Primary Control	Mechanism
L7 — Backup	DataDomain + S3 Glacier	Encrypted backup storage	Backup data encrypted in transit and at rest; access controls on DataDomain and AWS

4.2 Layer-by-Layer Security Controls

L1 — Internet Edge: Cloudflare

L1	Internet Edge	Cloudflare CDN / DDoS / WAF <i>All casinoglory.com DNS resolves to Cloudflare. Player traffic is inspected and filtered before reaching Primetel. Controls: DDoS mitigation (all sizes), Web Application Firewall (OWASP ruleset), IP reputation filtering, Bot management, SSL/TLS termination (TLS 1.2+), Rate limiting, Geo-blocking where required.</i>
-----------	----------------------	---

L2 — Perimeter: pfSense Firewall

L2	Perimeter	pfSense (VM on ESXi) <i>pfSense runs as a virtual machine on the ESXi cluster. Controls: Stateful packet inspection, NAT (hides internal IPs), Ingress/egress firewall rules, VPN for administrative remote access, Traffic logging for audit purposes.</i>
-----------	------------------	---

L3 — Network: Cisco Switch Cluster

L3	Network	Cisco Switch Cluster <i>Dual Cisco switches provide the internal LAN backbone. Controls: VLAN segmentation (Compute VLAN: 10.122.104.131 / Data VLAN: 10.122.120.120), Switch-level ACLs restricting inter-VLAN communication, Port security on all server-facing ports, Redundant dual-switch cluster eliminates single switch as a point of failure.</i>
-----------	----------------	--

L4 — Host: VMware ESXi Hypervisor

L4	Host	VMware ESXi (4x DELL PowerEdge R7625) <i>VMware ESXi provides hypervisor-level isolation between virtual machines. Controls: VM isolation (VMs cannot directly</i>
-----------	-------------	--

		access each other's memory or storage), ESXi host hardening (CIS VMware benchmarks applied), MFA on ESXi host management (vSphere/DCUI), RBAC on vSphere — only authorised personnel can manage VMs, Audit logging of all host management actions, Monthly patch review cycle for ESXi and VMware platform.
--	--	---

L5 — Application: Web Panels and Gaming Platform

L5	Application	Web Panels (x3) + Gaming Platform VM <i>Application-layer security controls: MFA enforced on all staff and administrative accounts, RBAC controls on all administrative functions (Operational Manual §5.2), Secure development principles applied to all platform code, Input validation and output encoding on all web-panel APIs, Fraud detection via the Risk Engine (monitors player behavior in real-time), AML/CFT transaction monitoring, Penetration testing annually and after significant changes.</i>
-----------	--------------------	---

L6 — Data: DELL PowerStore 1200T

L6	Data Layer	DELL PowerStore 1200T <i>Data-at-rest security: All production data encrypted at rest on PowerStore 1200T, All data encrypted in transit (TLS 1.2+), Role-based access controls on storage management — only authorised DBAs and admins can access storage management, Immutable audit logs maintained — logs cannot be altered or deleted, Tamper-evident records of all financial transactions and game outcomes.</i>
-----------	-------------------	---

L7 — Backup: DataDomain + Amazon S3 Glacier

L7	Backup	DELL DataDomain + Amazon S3 Glacier <i>Backup security: Veeam backup data stored on DELL DataDomain with deduplication and encryption, Amazon S3 Glacier backup data encrypted in transit (TLS) and at rest (AES-256), S3 Glacier access restricted to authorised AWS IAM roles only, Backup integrity verified on Veeam job completion, Quarterly restore testing validates backup data is readable and complete.</i>
-----------	---------------	--

4.3 Security Monitoring & Testing Schedule

Activity	Frequency	System / Scope
24/7 uptime and anomaly monitoring	Continuous	All ESXi hosts, pfSense, PowerStore, REDIS, web panels
AML/CFT transaction monitoring	Continuous	All player financial transactions
Cloudflare DDoS / WAF alert monitoring	Continuous	Cloudflare dashboard — all internet-facing traffic
pfSense firewall log review	Continuous (automated) + weekly manual	pfSense audit logs
ESXi host and VMware patch review	Monthly	All 4 ESXi hosts + VMware vSphere/ESXi platform
Vulnerability scans	Monthly + after major changes	Platform, network, application layer
Access control reviews	Quarterly	RBAC on all systems, ESXi, pfSense, storage, AWS
pfSense firewall configuration review	Quarterly	Firewall rules, NAT, VPN configuration
Penetration testing	Annually (minimum)	Full external and internal penetration test
Disaster recovery / security simulation	Annually	Full CMT exercise including cybersecurity scenario

SECTION 5

PAYMENT GATEWAY INTEGRATIONS

How payment processing connects to the platform and players

The Casino Glory platform accepts a range of payment methods from players. Payment processing is integrated through authorised and regulated payment service providers, connected to the platform via secure API integrations from the web-panel and gaming platform virtual machines.

5.1 Payment Architecture

Payment processing flows from the player browser, through Cloudflare and pfSense, to the web-panel API servers, which make outbound API calls to external payment service providers. Player wallet balances are stored persistently on the DELL PowerStore 1200T and cached in the REDIS cluster.

Component	Role	Location / Provider
Web Panel VMs (x3)	Originate outbound payment API calls; handle payment webhooks and callbacks	On-site: ESXi cluster, Primetel

Component	Role	Location / Provider
Gaming Platform VM	Processes wallet debits/credits; applies bonus engine to payment events	On-site: ESXi cluster, Primetel
REDIS Cluster	Caches active wallet state for real-time balance display; not authoritative	On-site: ESXi cluster, Primetel
DELL PowerStore 1200T	Authoritative persistent store for all player wallet balances and transactions	On-site: Primetel
pfSense Firewall	Routes outbound payment API traffic through Primetel ISP uplink	On-site: ESXi cluster (VM)
Primary Payment Gateway	External payment processor — primary route for deposits and withdrawals	[Provider]
Secondary Payment Gateway	External payment processor — fallback if primary is unavailable	[Provider]
Alternative Payment Methods	E-wallets, bank transfers, cryptocurrency where permitted	[Provider]

5.2 Payment Data Flow

1

Player Initiates Deposit / Withdrawal

Player submits payment request via casinoglory.com. Request passes through Cloudflare (WAF / DDoS filter) and pfSense firewall to the web-panel API tier.

2

KYC / Fraud / AML Checks

Web panel and Risk Engine validate the request: KYC verification status, fraud velocity checks, AML/CFT screening, payment method ownership verification, and account limit checks (Operational Manual §4.2, §4.3, §15.3).

3

Outbound API Call to Payment Gateway

The web-panel server makes an encrypted (TLS) outbound API call to the primary payment gateway via the Primetel ISP uplink and pfSense firewall. All payment API credentials are stored securely on the Gaming Platform / web-panel servers.

4

Payment Provider Processes Transaction

The payment provider processes the deposit or withdrawal with the player's bank, card network, or e-wallet. A callback/webhook is sent to the web-panel API confirming the outcome.

5

Wallet Update on PowerStore

On successful payment confirmation, the Gaming Platform updates the player's wallet balance on the authoritative PowerStore database and writes a transaction audit log entry. REDIS wallet cache is refreshed.

6

Confirmation Returned to Player

Payment outcome is returned through the web-panel API and Cloudflare to the player's browser. Failed payments are logged and the player is notified.

5.3 Payment Security Controls

- All payment API communications encrypted with TLS 1.2+ (in transit)
- Payment API credentials stored securely on platform — not exposed to player-facing systems
- Cloudflare WAF protects inbound payment callbacks/webhooks from spoofing or injection
- pfSense firewall controls outbound payment API traffic — only whitelisted payment provider IPs/domains permitted
- Daily reconciliation of player wallet balances against payment provider reports (Operational Manual §4.4)
- Player funds are administratively segregated from operational funds
- Automated fraud monitoring via Risk Engine on all transactions (Operational Manual §5.2)
- Enhanced due diligence applied to withdrawals exceeding defined thresholds (Operational Manual §4.3)
- All payment transactions logged with tamper-evident audit trail on PowerStore

5.4 Player Fund Protection

Player funds are administratively segregated from operational funds at all times . Daily reconciliations verify balances. Player wallet balances are persisted on DELL PowerStore 1200T and backed up via Veeam/DataDomain and Amazon S3 Glacier. A payment gateway or REDIS failure does NOT result in loss of player funds — PowerStore is the authoritative source of wallet state.

SECTION 6

BACKUP INFRASTRUCTURE

The License Holder maintains a three-tier backup strategy ensuring that all critical data can be recovered from multiple points at multiple geographic locations. This supports the Business Continuity Plan (BCP) recovery objectives and regulatory obligations for data retention.

T1
ON-SITE
VM
BACKUP**Veeam Backup & Replication → DELL DataDomain (PowerVault)****Frequency:** Per Veeam policy schedule (incremental daily, full weekly — to be confirmed)**Location:** On-site: Primetel Nicosia Datacenter

Veeam Backup & Replication captures VM-level image backups from the four ESXi hosts. Backup jobs read VM data from the PowerStore datastore and write deduplicated, compressed backup images to the DELL DataDomain (PowerVault) appliance. The DataDomain provides deduplication storage, reducing backup storage footprint. Veeam supports granular recovery of individual files, VMs, or application items from backup images.

- Coverage: All production VMs (pfSense, web-panels, gaming platform, REDIS, all databases)
- Recovery capability: Full VM restore, individual file restore, application-item restore
- Verification: Veeam backup job completion status verified daily

T2
ON-SITE
SNAPSHOT**DELL PowerStore 1200T — Hourly Storage Snapshots****Frequency:** Hourly**Location:** On-site: Primetel Nicosia Datacenter (PowerStore 1200T)

The DELL PowerStore 1200T generates hourly storage-level snapshots of all production volumes. These snapshots are space-efficient (copy-on-write) and provide the fastest recovery path for recent data — no VM restart required for data-layer recovery. Hourly snapshots deliver an RPO of ≤ 1 hour for storage-level failures or data corruption events.

- Coverage: All PowerStore volumes (VM datastores, databases, application data)
- Recovery capability: Rapid point-in-time volume restore or individual file/LUN clone
- RPO: ≤ 1 hour (most recent snapshot within the last 60 minutes)
- RTO: Fast — PowerStore snapshot restore is typically < 30 minutes for volume-level recovery
- Verification: PowerStore snapshot completion verified daily

T3
OFFSITE
COLD**Amazon S3 Glacier — Offsite Long-Term Backup****Frequency:** Per replication schedule (from DataDomain / Veeam export)**Location:** Offsite: Amazon AWS S3 Glacier (geographically separate from Primetel Nicosia)

Backup data is replicated from the on-site DataDomain / Veeam infrastructure to Amazon S3 Glacier for long-term offsite cold storage. Amazon S3 Glacier provides the geographic separation required for disaster recovery scenarios where the Primetel Nicosia Datacenter is wholly unavailable. S3 Glacier also satisfies long-term regulatory data retention obligations.

- Coverage: All critical backup data from DataDomain / Veeam exports
- Recovery use case: Full datacenter loss at Primetel — primary DR recovery path when all on-site infrastructure is unavailable

- Retrieval time: Standard retrieval: 3–5 hours. Expedited retrieval: 1–5 minutes (for objects < 250 MB). Plan retrieval timelines in advance for DR scenarios.
- Retention: Long-term retention per Curaçao AML/CFT obligations and regulatory recordkeeping requirements
- Encryption: Data encrypted in transit (TLS) and at rest (AES-256) on S3 Glacier
- Access: Restricted to authorised AWS IAM roles only

6.1 Backup Data Inventory & Retention

Data Type	Backup Tiers	Retention Period	Regulatory Basis
Player account & wallet data	T1 (Veeam) + T2 (Snapshot) + T3 (Glacier)	7+ years	Curaçao AML/CFT obligations
Transaction records (deposits/withdrawals)	T1 + T2 + T3	7+ years	Regulatory recordkeeping requirements
Game round logs and RNG outcomes	T1 + T2 + T3	Per regulatory requirements	Curaçao gaming legislation (LOK)
Audit logs (system, financial, security)	T3 (Glacier) — immutable	Per regulatory requirements	Operational Manual § 14.3 — immutable logs
KYC and AML/CFT records	T1 + T3	Per AML legislation	AML/CFT obligations
pfSense firewall configuration	T1 (Veeam)	Operational continuity	BCP recovery requirement
ESXi host configurations	T1 (Veeam)	Operational continuity	BCP recovery requirement
REDIS session cache	T1 (Veeam)	Operational — recreatable	Non-authoritative; rebuilt from DB on restart

6.2 Backup Recovery Priority Order

In a recovery scenario, the following priority order applies:

Priority	Source	When to Use	Estimated RTO
1st	DELL PowerStore 1200T — Hourly Snapshot	Data corruption or storage-level failure; on-site infrastructure available	< 1 hour
2nd	Veeam Backup on DELL DataDomain	VM-level failure; host failure; PowerStore snapshot not suitable	1–4 hours

Priority	Source	When to Use	Estimated RTO
3rd	Amazon S3 Glacier	Full datacenter loss; both on-site backup systems unavailable	4–8+ hours (plus compute provisioning time)

SECTION 7

REDUNDANCY ARCHITECTURE

The Casino Glory infrastructure incorporates redundancy at multiple layers to minimise single points of failure and support the Recovery Time Objectives (RTOs) defined in the Business Continuity Plan. The following summarises the redundancy posture at each layer.

7.1 Layer-by-Layer Redundancy Summary

Network Layer — Cisco Switch Cluster

Component	Redundancy Type	Failure Scenario	Expected Impact
Cisco Core Switch 1 + Switch 2 (cluster)	Active-active dual switch cluster (10.122.120.200)	Single switch failure	Automatic failover to surviving switch — expected zero downtime
Physical cabling	Dual NIC — each ESXi server has one connection to each switch	Single cable or NIC failure	Surviving connection maintains connectivity — expected zero downtime

The dual Cisco switch cluster is the strongest redundancy component in the architecture. A single switch failure is fully absorbed with no expected service interruption.

Compute Layer — VMware ESXi Cluster (4 Nodes)

Scenario	Redundancy Mechanism	Expected Impact	Manual Action Required
Single ESXi host failure (1 of 4)	VMware HA auto-restarts affected VMs on surviving hosts	Brief VM restart (minutes); no data loss	Monitor HA; verify VM restart; contact DELL for host repair
Two ESXi host failures simultaneously	VMware HA — may have insufficient capacity for all VMs	Potential service degradation on non-critical VMs	Manually prioritise critical VM restarts on surviving 2 hosts

Scenario	Redundancy Mechanism	Expected Impact	Manual Action Required
All 4 ESXi hosts failed (datacenter loss)	No on-site compute redundancy	Full platform outage	Emergency cloud compute provisioning from S3 Glacier recovery

Application Layer — Web Panels (3 Instances)

Scenario	Redundancy Mechanism	Expected Impact
Single web-panel VM failure (1 of 3)	2 remaining web-panel VMs continue serving traffic	Reduced capacity but service maintained
Two web-panel failures (2 of 3)	1 remaining web-panel VM serves all traffic	Degraded performance but service likely maintained
All 3 web-panel failures	No web-panel redundancy — dependent on ESXi HA restart	Service unavailable until VM restart on surviving ESXi hosts

Three web-panel instances provide application-level redundancy for the API tier. A load balancer or reverse proxy should be configured to distribute traffic across all three and detect/remove failed instances automatically.

Storage Layer — DELL PowerStore 1200T

Scenario	Redundancy Mechanism	Expected Impact
Single drive failure	PowerStore internal RAID / drive rebuild	Self-healing; no service impact expected
Dual controller failure	PowerStore dual-controller architecture (if configured)	Controller failover; brief I/O pause expected
Full PowerStore failure	No second SAN; must restore from Veeam/DataDomain or Glacier	Major outage; 1–4 hour recovery from Veeam; 4–8+ hours from Glacier

CDN / DDoS Layer — Cloudflare

Scenario	Redundancy Mechanism	Expected Impact
Cloudflare global incident	Cloudflare anycast network is globally distributed across 200+ data centers	Cloudflare has extremely high availability; true global outage is rare and brief
DNS misconfiguration	Cloudflare DNS is managed via dashboard; rollback available	Player access issues until DNS corrected — minutes to hours

Scenario	Redundancy Mechanism	Expected Impact
Primetel datacenter offline	Cloudflare can route to alternative origin if configured	Requires pre-configured failover origin; otherwise players see Cloudflare error page

Backup Layer — Three-Tier

Tier	Redundancy	Geographic Separation
Tier 1 — Veeam / DataDomain	On-site VM backup; survives VM/host failures and data corruption	No — same datacenter as production (Primetel Nicosia)
Tier 2 — PowerStore Snapshots	On-site snapshots; survives application-level data corruption	No — same datacenter as production (Primetel Nicosia)
Tier 3 — Amazon S3 Glacier	Offsite cold storage; survives full datacenter loss	YES — Amazon AWS (geographically separate from Primetel Nicosia)

Annex B Third party providers

SECTION 8

COMPLETE INFRASTRUCTURE SUMMARY

Layer	Component	Model / Provider	Function
Internet / CDN	Cloudflare CDN / DDoS / WAF	Cloudflare	Player traffic filter; CDN; DDoS; WAF; SSL termination
ISP	Primetel Public IPs	Primetel (Cyprus ISP)	Internet ingress/egress for Primetel Nicosia Datacenter
Firewall	pfSense (VM)	pfSense on VMware ESXi	Stateful firewall, NAT, traffic routing
Network	Cisco Core Switch 1 (cluster)	Cisco Switch	Redundant switch cluster — node 1 of 2
Network	Cisco Core Switch 2 (cluster)	Cisco Switch	Redundant switch cluster — node 2 of 2
Network	LAN Segment A (Compute VLAN)	VLAN	Internal compute network segment
Network	LAN Segment B (Data VLAN)	VLAN	Internal data/storage network segment
Compute	ESXi Host 1	DELL PowerEdge R7625	VMware ESXi virtualisation host
Compute	ESXi Host 2	DELL PowerEdge R7625	VMware ESXi virtualisation host
Compute	ESXi Host 3	DELL PowerEdge R7625	VMware ESXi virtualisation host
Compute	ESXi Host 4	DELL PowerEdge R7625	VMware ESXi virtualisation host
Application	web-panel-1	VM on ESXi	Front-end web server / API tier (1 of 3)
Application	web-panel-2	VM on ESXi	Front-end web server / API tier (2 of 3)
Application	web-panel-3	VM on ESXi	Front-end web server / API tier (3 of 3)
Application	Gaming Platform VM	VM on ESXi	Casino Glory core engine; bonus; risk; RNG; admin backend
Application	REDIS Production Cluster	VM on ESXi	Session cache; real-time game state; wallet cache

Layer	Component	Model / Provider	Function
Application	Static Assets Service	VM on ESXi	Serves static game content assets
Storage	DELL PowerStore 1200T (Primary SAN)	DELL PowerStore 1200T	Primary SAN for all ESXi VM datastores and databases
Backup (on-site)	DELL DataDomain (PowerVault)	DELL DataDomain	Veeam backup target; deduplication appliance
Backup (on-site)	PowerStore Hourly Snapshots	DELL PowerStore 1200T	Hourly storage snapshots for rapid point-in-time recovery
Backup (offsite)	Amazon S3 Glacier	Amazon AWS	Long-term offsite cold storage; disaster recovery backup

Appendix C –Terms and Conditions

Website Terms and Conditions

Effective from: Aug 2025

Last updated: Aug 2025

Version: 1.0

Date: Aug 2025

DEFINITIONS

The following words and terms, when used in these Terms shall have the following meanings, unless the context clearly indicates otherwise:

Account Holder:

An individual who applied and was granted a Player Account on the Website.

ADR Notice

Notice in writing by the Player or Company to the other party, referring a Dispute to mediation.

ADR:

Alternative dispute resolution ('ADR')

AML:

Anti-Money Laundering. All efforts focused on the prevention of transforming proceeds obtained from criminal activities into funds which appear to be obtained from legal activities.

CFT:

Combating the Finance of Terrorism. All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.

The Company:

GMFY Tech N.V., a limited liability company incorporated under the laws of Curaçao, having its address at Groot Kwartierweg 10, Livestrong Building, Curaçao and registered in the Commercial Register of the Curaçao Chamber of Commerce and Industry under number # 148776

Customer Support Team

The Company's team of employees who provide help when Account Holders have trouble with the Services.

Complaint:

Complaint on the performance of the Company under the agreement governed by the Terms from the Player.

Curacao Gaming Authority

The authority from which the Company has obtained its gaming license.

Games:

Any games available on the Website and as may from time to time become available on the Website.

Identification

The collection of a series of personal details of the prospective Account Holder. Identification is the first step in the KYC process.

KYC:

Know Your Client: the mandatory process of identifying and verifying a prospective Account Holder's identity when opening a Player Account and periodically over time.

Multi-accounting

When one Player Account Holder has more than one Player Account, or if there are more than one Player Accounts registered per IP address or Shared Environment. Multi-accounting mainly manifests by similar IP addresses for different Player Accounts. Multi-accounting is forbidden as it impairs AML measures that the Company takes in order to combat money laundering or terrorist financing.

Player:

Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened providing him/her with a unique code.

Player Account:

An account granted to an individual after registration on the Website. The Player Account is created and issued by the Company. Only one Player Account is permitted per person, per IP address, and per Shared Environment.

Restricted Jurisdictions

Jurisdictions of which the residents are prohibited to register on the Website and make use of the Services.

Restricted Jurisdictions List

List containing all Restricted Jurisdictions. Currently the following Restricted Jurisdictions are on the Restricted Jurisdictions List: Aruba, Australia, Bonaire, Belgium, Curaçao, France, Netherlands, Saba, Singapore, Sint Maarten, Spain, Statia, U.K., U.S.A or the U.S.A dependencies.

Shared Environment:

An environment that has a common internet connection which can be used by multiple persons, including but not limited to households, airplanes, universities, libraries, cyber cafes, coffee shops and work forces. Only one Player Account is permitted per Shared Environment.

Service:

Any gaming and betting offer provided by the Company to the Account Holder through the Website.

Software

Any computer program, data file or any other content that may be required to be installed on the Player's device to enable the Player to use, access and participate in the Services for the purpose

of using, accessing, and participating in the foregoing on the Website and all software available on the Website.

Terms:

These Terms and Conditions, the Company's Privacy Policy, the Company's Cookies Policy and any other rules applicable to the Company's betting or gaming products available on the Website.

Verification Checks:

Checks performed to verify the Player's identity as described in article 6.

VIP Manager

Employee of the Company, charged with the communication with Players who are eligible, and/or have applied for and/or have obtained a VIP status.

Website:

Any part of Company's website and or any sub-domain, website, or mobile application that the Company owns or operates under its e-gaming sub-license.

Website Material:

The Website and all content and Software made available on it.

1 GENERAL

By using, visiting and/or accessing the Website and/or registering a Player Account, the Player agrees to be bound by the Terms and is deemed to have accepted and understood all the Terms.

2 CHANGES TO TERMS

The Company reserves the right to unilaterally change the Terms when such need occurs. The Company will do its best to notify Players of any significant changes by email. However, the Company does recommend all Players to revisit this page regularly and check for possible changes. If the Player continues to use the Website after such changes come into effect the Player is deemed to have accepted such changes to the Terms.

3 ACCOUNT

3.1 By registering a Player Account, the Player declares that he/she is over 18 years of age or of a higher minimum legal age as stipulated in the jurisdiction of the Player's residence under the laws applicable to the Player. It is the Player's sole responsibility to know whether the Services are legal in the country of the Player's residence. Persons who are under the age of 18 years are not allowed to use the Website and/or any Services available on it.

3.2 By opening a Player Account and/or by using the Website, the Player acknowledges, agrees, and confirms the following:

- a) The Player is at least 18 years of age and above the legal age for gambling in the Player's jurisdiction of residence.
- b) The Player is legally capable of entering into binding contracts.
- c) The Player has supplied correct and materially complete information when registering with the Website, will ensure that such information is kept updated throughout his/her use of the Website, and acknowledges that failure to do so willfully may lead to the Company forfeiting all the Player's winnings.
- d) The Player resides at the address the Player provides to the Company.
- e) The Player does not reside in a Restricted Jurisdiction.
- f) The Player resides in a territory that permits gambling, acknowledging that it is the Player's sole responsibility to inform himself about the rules in his/her country of residence that may prohibit the Player from registering and/or wagering on the Website.

- g) The Player has not excluded himself/herself from gambling on this Website or any other website operated by the Company.
- h) The Player has a valid bank account or credit or debit card or alternative payment method.
- i) The Player is the legitimate owner of the money the Player deposits and any money that the Player deposits into his/her Player Account is not tainted with any illegality and does not originate from any illegal activity or source.
- j) The Player has no existing Player Account registered on the Website.
- k) The Player makes use of the Services strictly in his/her personal non-professional capacity, on his/her own behalf and expressly not on the behalf of any other person or company.
- l) The Player will not sell, transfer and/or acquire Player Accounts to/from other Players.
- m) The Player participates on the Website for fun and not for financial dependency (or similar) reasons.
- n) The Player will comply with the Terms at all times in relation to his/her use of the Website.
- o) The Player will use the Website and the Player Account solely for the purpose of his/her genuine participation in the Games.
- p) The Player acknowledges that there is a risk of losing money when gambling through the Website and is fully responsible for any such loss.

Upon the suspicion of any use of the Website in breach of this article, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close the Player Accounts involved.

3.3 By opening a Player Account, the Player consents to the Company contacting the Player through any and all means of communication (whether in written or verbal form and including, but not limited to email, telephone and SMS) in respect to matters relating to his/her Player Account.

3.4 In the event of any of the warranties outlined in 3.2 being false, the Player's stake will be forfeited, and the Company shall not be obliged to pay any winnings and/or deposits. The Company may also report the matter to the police, parents (in relation to underage gambling) and the appropriate regulatory authority.

3.5 The Company may decline acceptance of an account application at any time and for any reason.

3.6 From time to time the Company offers promotions for new Player Accounts. Registered Players are not eligible to register a new Player Account. Registration of a new Player Account by a registered Player is prohibited and considered as an example of Multi-accounting.

3.7 Employees of the Company, its licensees, distributors, wholesalers, subsidiaries, advertising, promotion or other agencies, media partners, retailers and members of the immediate families of each are not eligible to participate in the Games.

4 RESTRICTED JURISDICTIONS

4.1 Residents of Restricted Jurisdictions are not allowed to register on the Website and use the Services.

4.2 The Company reserves the right to refuse customers from any other jurisdictions over and above the Restricted Jurisdictions at its own discretion.

4.3 The Company reserves the right to amend the Restricted Jurisdictions List from time to time and at the Company's sole discretion. The Player shall be informed by email about such amendment.

4.4 The Player Account of any Player who opens the Website while residing in a Restricted Jurisdiction may be closed by the Company immediately upon detection thereof. Any winnings

and bonuses obtained by the Player from the time the Player opened the Website while residing in a Restricted Jurisdiction will be confiscated, and the remaining balance on the Player's Account shall be returned subject to the deduction of any payment processing charges. Any winnings or bonuses which the Player has gained or accrued after the Player opened the Website while residing in the Restricted Jurisdiction will be forfeited by the Player and may be reclaimed by the Company. The Player will return to the Company on demand any such funds which have been withdrawn.

4.5 Maximum of two weeks prior to the placement of a jurisdiction on the Restricted Jurisdictions List, such placement will be announced on the Website. Any Player who resides in such jurisdiction or has his registered address in such jurisdiction will be informed (by email) by the Company of the Company's intention to place said jurisdiction on the Restricted Jurisdictions List, the date of such placement, as well as the intended closure of such Player Account upon the placement. The Player is granted the opportunity to withdraw remaining funds on his/her Player Account until the closure of the Player Account. In case there are any funds remaining on the Player Account at moment of closure of the Player Account, the Player may request the Customer Support Team to assist with the transfer of such funds to the Player in accordance with article 9.

4.6 It is the Player's sole responsibility to inform themselves about the rules in their country that may prohibit them from registering and/or wagering on the Website.

4.7 The availability of the Website in a certain jurisdiction does not constitute an offer, solicitation, or invitation by the Company for the use of betting, gaming or other services in any jurisdictions in which such activities are prohibited by law. Under no circumstances will the Company be liable for any breach of state or country law that may occur as a result of the Player's usage of the Website.

5 IDENTIFICATION

5.1 By opening a Player Account, the Player agrees that as part of the KYC in the account opening process, Identification shall take place. Identification is the first step in the KYC process. The prospective Account Holder is requested to provide the following details:

- a) name and surname;
- b) permanent residential address;
- c) date of birth;
- d) place of birth;
- e) nationality; and
- f) identity number.

5.2 The Company reserves the right to close, suspend or terminate a Player Account at its sole discretion if there is any issue with the Identification.

6 VERIFICATION CHECKS

6.1 The Player furthermore agrees that the Company may perform Verification Checks as described in further detail in this article. The Company reserves the right to close, suspend or

terminate a Player Account at its sole discretion if there is any issue with the Verification Checks.

6.2 The Player may be asked to verify the Player's email via an activation link or other proof that the email account belongs to the Player. If this step is not completed, the Player Account may be suspended, and any winnings voided until the Player Account details have been verified.

6.3 Electronic age verification checks are carried out and the Company may make use of third-party agencies to confirm the Player's age. The Company may require and request further information directly from the Player. If, upon completion of Verification Checks (or subsequently) the Player is ultimately proven to be underage: (i) his/her Player Account will be closed; (ii) any winnings obtained while using the Website will be retained by the Company; and (iii) all funds deposited by the Player will be returned by a method determined by the Company. Any monies already withdrawn will be deducted from the amount returned.

6.4 The Company may make use of third-party agencies to confirm the Player's age, identity, address, payment details and methods or any other information that the Player provides to the Company. This process will involve checking the disclosed details against certain (public or private) databases. By entering this process, the Player agrees that the Company may use, record, and disclose such personal information and this data may be recorded by the Company or them. The third parties that the Company uses are fully aware of its obligations applicable data privacy legislation and will always act in accordance with its provisions and the Company's instructions.

6.5 As part of the Verification Checks, there may be requests for supporting ID or other documentation or information which the Player will be advised of at the time. The Company may suspend the Player Account and/or prevent the Player from placing any further bets until the Player has satisfactorily completed these Verification Checks.

6.6 The Company may decide to carry out further Verification Checks (including requesting extra documents or information) to confirm, without limitation, the Player's identity, age and address or payment method details at any time. This is to satisfy the Company's license obligations, routine security checks and to safeguard the integrity of the relevant Player Account.

6.7 If, upon completion of Verification Checks, the Company is unable to verify the Player's details or the Player is unable and/or unwilling to provide proof of his/her residential address, or other information required to complete verification, the Company will within a reasonable time (i) close the Player Account; and (ii) return any residual balance, up to the value of the Player's initial deposits, at the time of the unsuccessful verification. Any winnings after the unsuccessful verification will not be credited.

6.8 In addition to the above and as part of the Company's compliance with AML regulations, the Company may at any time (including, but not limited to, certain stages of the Player Account registration) ask the Player to not only verify the Player's identity and address but also request proof of ownership for any payment methods used to deposit or withdraw funds. In addition, the Company at any moment may request proof of the Player's source of funds and/or source of wealth.

7 USE OF THE WEBSITE

7.1 Access to the Website is permitted on a temporary "as is" basis, and the Company reserves the right to withdraw, suspend or amend any aspect or feature of the Website without any notice. If the need arises, the Company may suspend access the Website or to parts thereof for maintenance purposes. The Company will not be liable if, for any reason, the Website is unavailable at any time or for any period.

7.2 The Company may, in its absolute discretion, change, amend, withdraw, add the Website Material (including Games, betting products or elements of the betting product) of the Website at any time without notice (provided such changes do not affect games and/or bets already in progress). The Company shall not be liable to the Player for any loss suffered because of any changes made or for any modification or suspension of or discontinuance of the Software or Service and the Player shall have no claims against the Company in such regard.

7.3 The Player shall use the Website for the Player's own personal, domestic and noncommercial use only and shall not be allowed to provide access or reproduce the Website or any part of it in any form whatsoever without the Company's express consent, including creating links to it.

7.4 The Player shall not use the Website for any purpose which is or is likely to be considered to be defamatory, abusive, obscene, unlawful, of a racist, sexist or other discriminatory nature, or which could cause offence.

7.5 The Player must not misuse the Website by knowingly introducing viruses, trojans, worms, logic bombs or other material which is malicious or technologically harmful. The Player must not attempt to gain unauthorized access to the Website. The Company cannot guarantee that the Website will be compatible with any hardware or software that may be used by Players.

7.6 The Player is solely responsible for making all arrangements necessary for the Player to have access to the Website. The Company will not be liable for any losses caused to the Player by the internet or any telecommunications service provider which the Player have engaged in order to access the Website.

7.7 If the Player wants to report an error or have any questions, the Player should contact the Customer Support Team. Please note that any calls to the Customer Support Team may be monitored and/or recorded (of which the Player will be notified at the beginning of the call if it is being recorded or monitored) for training and quality management purposes and to assist the Company in quick and effective resolution of queries.

8 MAINTAINING THE PLAYER'S ACCOUNT

8.1 Opening of more than one Player Account by a Player or by multiple Players in a Shared Environment is considered Multi-accounting and is strictly prohibited. When there are more than one Player Accounts registered per IP address or Shared Environment, all Player Accounts opened after the first Player Account registered on the IP address shall be considered to be in breach of the prohibition on Multi-accounting. The prohibition on Multi-accounting has several reasons, such as prevention of collusion, affiliate fraud and AML: Multi-accounting can be used for chip dumping, where a Player uses one of their Player Accounts to deliberately lose its chips to another Player Account, in order to launder money.

8.2 In case of detection of Multi-accounting, the Company has the right to close the Player Account(s) and cancel the bonuses offered and/or winnings, if any. Once completed, any remaining funds may be returned to the Player(s) subject to the deduction of any payment processing charges and administrative charges.

8.3 When opening a Player Account, the Player is requested to choose his/her own username and password. The Player should ensure that these details are kept safe and private, as the Player is responsible for all bets placed on his/her Player Account, where the correct security information has been provided. If the Player loses, or forgets, his/her username and/or password, or if the Player believes that a third party is aware of them, the Player should contact the Company immediately so that new security details can be allocated to the Player. These new details will be emailed to the Player.

8.4 If another person accesses a Player Account, the Player is solely responsible for all their actions whether or not their access was authorized by the Player as it is the Player's sole obligation to store the log-in details of his/her Player Account in a safe and private manner. The Player hereby indemnifies the Company and holds the Company harmless against all costs, claims, expenses and damages arising in connection with the use of or access to the Player Account by any third party.

9 ACCOUNT FUNDS, DEPOSITS AND WITHDRAWALS

9.1 The Company holds Players funds for all Players (irrespective of location) separate from the Company's funds in a separate bank account which is used for Player funds only.

9.2 The Player declares with each deposit that the to be deposited funds rightfully belong to the Player and that these funds have not been obtained or are derived from any illegal means. The Company retains the right to request additional source of funds based on a case-by-case basis.

9.3 The maximum amount the Player is allowed to deposit per day/ 24 hours is EUR/USD 5.000 (or the equivalent in the Player Account currency). Any deposits above said maximum amount may be cancelled and returned by the Company.

9.4 The Company has the right to request the Player to provide to the Company source of funds when the Player makes/has made a deposit of an amount greater than EUR/USD 2.000 in 24 hrs (or the equivalent in the Player Account currency).

9.5 Deposits to the Player Account are made by transfer of money to the Player Account by way of the payment methods stated on the 'Deposit' page upon login to the Player Account.

9.6 The Company reserves the right to change the forms of payment that it may accept from time to time.

9.7 The Player may only use payment methods registered in the Player's own name to make deposits and withdrawals.

9.8 The Company reserves the right to accept certain methods of payment only subject to the fulfilment of certain conditions.

9.9 The Company does not warrant that all methods of payment are always available.

9.10 The Company does not accept cash funds sent to the Company.

9.11 The transfer of funds between Player Accounts on the Website is prohibited.

9.12 By depositing money, the Player agrees not to make any chargebacks, reversals or otherwise cancel any deposits into his/her Player Account and agrees to refund and compensate the Company for unpaid deposits.

9.13 The Company accepts no responsibility for any currency exchange conversions, charges or fees levied by the Player's card issuer, bank or financial institution.

9.14 As the Company's products are consumed instantly when playing or betting, the Company cannot provide returns of goods, refunds or cancellation of the Player's Service when playing or betting. If the Player plays a Game or uses a Service with money, the money can be drawn from his/her Player Account instantly.

9.15 A Player Account should not be used as a banking facility/account. Player Accounts are not insured, guaranteed, sponsored or otherwise by any banking insurance system nor shall they earn any interest. Deposits should only be made with a view to using funds to place bets. Should the Player make deposits and withdrawals without wagering, the Company reserves the right to block the funds on the Player Account until further notice.

9.16 The Player's credit card, debit card or e-wallet will be billed immediately after purchase. For queries regarding billing descriptors on the Player's statements, the Player may contact the

Customer Support Team. The Company bears no responsibility for the billing descriptors used by the payment service provider used by the Player.

9.17 No withdrawal will be processed, and funds cannot be withdrawn from a Player Account until: (i) Identification and Verification Checks have been satisfactorily completed; (ii) payments have been confirmed; and (iii) the Player has complied with any other withdrawal conditions, specific rules and promotional terms relating to the Player's use of the Website and/or affecting his/her Player Account (for example, any applicable bonus terms), and (iv) wagering activity has been conducted by the Player in the minimum amount of 1 x deposit value of the player for slot games and 2x deposit value on table games before requesting withdrawal. Please note that Verification Checks include checks on the Player's identity, age, place of residence and proof of ownership for any payment methods used (including the source of the Player's funds or wealth) as further set out in article 6. The Company may withhold any withdrawal in instances where the Player have not complied with any of the conditions in this article.

9.18 Should the Player wish to withdraw some or all of the balance on his/her Player Account, the Player may select how much the Player wish to have paid back, which amount however may not exceed maximum the withdrawal amount as defined in article 9.25, nor the maximum amount set by the payment method chosen by the Player when placing a deposit.

9.19 All withdrawals must be done through the same payment method and payment details, chosen by the Player when placing a deposit, unless the Company is unable to do so or decides otherwise. The withdrawal methods will become available once a successful deposit is made with such method.

9.20 Where the Player's withdrawal method is no longer valid or available (for example, it has expired) the Player's withdrawal will not be processed, and the Player will be asked for details of an alternative payment method. The Company may request further information or documentation from the Player in this instance.

9.21 Once a withdrawal is requested, it will remain pending for between 1-2 days. Once approved it will be processed immediately but may take up to 5 working days to reach the Player's account - this period will vary depending on the withdrawal method selected.

9.22 The minimum withdrawal is EUR/USD 20,-. To make a withdrawal, the Player must have wagered at least once, in full, the deposited amount.

9.23 Unless otherwise agreed in writing, the maximum amount the Player may withdraw in any week is EUR/USD 10.000 weekly. Players who have obtained the VIP status may be eligible for a withdrawal limit increase and may request such increase by contacting the VIP Manager. In case the Company agrees to a withdrawal limit increase, this shall be confirmed in an e-mail from the VIP Manager to the Player.

9.24 All withdrawals must be done through the same payment method and payment details, chosen by the Player when placing a deposit, unless the Company is unable to do so or decides otherwise. This is at the Company's discretion. If the Player has deposited using several payment methods, the Company reserves the right to split the Player's withdrawal across such payment methods and process each part through the respective payment method at the Company's discretion and in accordance with AML policies and regulations.

9.25 The Player agrees that all deposits/withdrawals made to/from the Player's Account, are transferred to/from bank account/s, debit/credit card/s, wallet or any other payment options available in the Player's country, which belong solely to the Player and are in the Player's name. It is prohibited to make any withdrawal from a Player Account, bank account/s, debit/credit card/s, wallet or any other payment options which do not belong (solely) to the Player. This is to

prevent that the Company transfers funds to persons who have not been duly identified by the Company, in accordance with AML policies and regulations.

9.26 The Player may only withdraw the maximum amount of EUR/USD 2.000 (or the equivalent in the Player Account currency) in any twenty-four-hour period unless a larger amount has been agreed upon between the Player and the Company. The Company may reject a withdrawal request if the suspicion arises that funds are being withdrawn for any fraudulent or money laundering reasons, pending the investigation thereto. Notwithstanding the maximum withdrawal amount as defined in this article, the maximum withdrawal amount is limited by the limitations set by the payment method chosen by the Player when placing a deposit.

9.27 Funds may be deducted from withdrawals in compliance with and as required by any applicable regulation or law.

9.28 If the Company mistakenly credits a Player Account with winnings that do not belong to the relevant Player, whether due to a technical error, error in the pay-tables, or human error or otherwise, the amount will remain property of the Company and the amount will be deducted from the Player Account. If the Player has used any such amount to place wagers, the Company may cancel these wagers and void any winnings. If the Player has withdrawn funds that do not belong to the Player prior to the Company becoming aware of the error, the mistakenly paid amount will (without prejudice to other remedies and actions that may be available at law) constitute a debt owed by the Player to the Company and the Company may take steps to recover such amount. In the event of an incorrect crediting, the Player is obliged to notify the Company immediately by email.

9.29 All transactions shall be checked to prevent money laundering. The Company shall report any suspicious transactions to the relevant competent authorities in Curaçao and/or the country the Player is based in. If the Player become aware of any suspicious activity relating to any of the Games or anything relating to the Website, the Player must report this to the Company immediately. The Company may suspend, block or close a Player Account and withhold funds if requested to do so in accordance with applicable law.

9.30 Enhanced due diligence may be performed in respect of withdrawals of funds not used for wagering.

10 PAYMENTS OF WINNINGS

10.1 Returns due on bets placed will be added to the Player's current deposit balance once the bet has been settled. This balance will remain in the Player Account unless the Player submits a request that part, or all, of the outstanding balance is returned to the Player. If the Player's balance is zero, the Player will be required to transfer more funds before the Player are able to place any bets. The Company does not offer any form of credit at any time.

10.2 The Player's processed funds will leave the Company at the end of each working day that the chosen payment method is open (considering local national holidays in the country of incorporation of the payment service provider) and the timing for processing will vary depending on the time as well as the country and financial institution in question.

10.3 Payment of winnings may be subject to further Verification Checks as set out in article 6.

10.4 The maximum winnings amount per 24 hours is EUR/USD 100.000 (or the equivalent in the Player Account currency), any winnings above said maximum amount may be cancelled by the Company. The reason for this limitation is some Games have for example free spins bonus games on which the bonus free spins can be re-triggered, and an unlimited number of times too. The maximum winnings amount is in place to limit the amount of cash a Player could win if the bonus game triggering symbols keep on spinning in during the bonus game and keep re-

triggering the bonus game too. In case the maximum daily winnings amount is reached, the Player understands and accepts that no further winnings can be added for that day, after the Player continues to play.

10.5 With due consideration of amount set in article 10.4, if the Player wins [amount] or more, the Company reserves the right to divide the payout into ten instalments, paid as 10 per cent every month for 10 months until the full amount is paid out. The Player will not get any interest on outstanding amounts and the Player shall not treat the Company as a financial institution.

10.6 If required, it will remain the Player's responsibility to report any winnings and losses to the Player's local law, regulatory, or tax authorities or any other relevant authorities. The Company will not be liable to such authorities for any payment of the Player's personal taxes. Please note that regulatory changes in respect of taxation in certain jurisdictions may have an impact on these Terms and may include the deduction of any applicable levy from the Player's winnings or withdrawals.

11 CURRENCIES AND CURRENCY ARBITRAGE

11.1 Players must register and play in the currency of their country or in cryptocurrencies. If the currency of the Player's country is not offered, then Euros (EUR) should be used. In case the Player does not observe this rule, all winnings derived from the resulting game play will be forfeited.

11.2 Players are strictly prohibited from utilizing the Website and its systems to facilitate arbitrage through currency exchange transactions. Where the Company deems in its sole discretion that a Player has deliberately used said systems for financial gain through arbitrage, any gains will be forfeited and deducted from the Player's balance without warning or notification.

11.3 If Games are available for the Player to play in a currency which is different to the currency of his/her Player Account, then to play them the Player may add a second currency to his/her Player Account. Alternatively, the Player can simply attempt to join a Game in the currency the Player would like to add, and the Company will automatically add the currency and make the conversion for the Player. With automatic conversion selected, any time that a currency conversion is required it will be performed automatically, and the Player will not be notified. A minimum conversion amount will apply, as set out on the Website.

11.4 All currency conversions made via the Website will take place at the current prevailing rate that the Company offers for the transaction type in question (this will be notified to the Player on the Website when the Player makes a conversion). Where currency conversion is available, the rate of exchange the Company offers is [insert exchange rate] plus a small margin (though the Company may, at its discretion, waive the margin for some types of transactions). The conversion rates will be updated on a regular basis, and it is possible that different rates may be offered depending on the type of transaction and movement in currency value. The Company may, in its own discretion, revoke or withdraw support for any particular currency without notice.

11.5 When currency is converted, any cancelled or rejected withdrawals from the Player Account will be returned to the Player in the currency and amount the Player originally requested, not the converted amount (for example, if Player Account is in EUR and Player tried to withdraw EUR 100 converted to USD, EUR 100 will be returned to the Player Account). Any cancelled or rejected deposits to the Player Account will be debited from the Player Account in the converted amount (for example, if the Player Account is in EUR and the Player made a deposit in USD, the EUR value will be debited from the Player Account), and if the Player does not have enough

funds in his/her Player Account to cover the debited amount, the Player will need to top up his/her Player Account.

11.6 The Player should be aware of fluctuations in the exchange rate and the impact this could have on the Player's available funds. Where currency conversion is available for the Player Account, it is the Player's responsibility to check the applicable rates before proceeding with transactions involving currency conversion. The Company is not responsible for gains or losses incurred by making currency conversions through the Services.

11.7 The Company is not a currency exchange. Where available, currency conversion via the Player Account is only to facilitate genuine gameplay. The Player must not use his/her Player Account or any other part of the Website to engage in currency trading, speculation or arbitrage.

11.8 The Company will take action to help maintain the integrity of any available currency conversion facilities. This could include:

- a) declining or reversing any currency conversion transactions made via a Player Account;
- b) limiting the number of currencies held in the Player Account and/or the amount of money that the Player may convert between currencies;
- c) requiring any converted funds in the Player Account to be used for playing Games before being withdrawn, transferred (where transfers are available) or used for any other purpose; and/or
- d) retroactively applying any margin which was waived as part of a currency conversion transaction.]

12 PROGRESSIVE JACKPOT WINS

The maximum amount set art. 10.4 does not include progressive jackpot winnings does not include any potential progressive jackpot winnings. The Player acknowledges and agrees that for certain products the Player's approved staking level may mean that the Player can win more than the amount set out above, and that the Company shall only be obliged to pay to the Player the maximum amount specified above.

13 BONUSES

13.1 Bonuses are promotions created for the Players. Only Players with a unique IP address can benefit from the Company's bonuses. For this reason, if a Player logs in to the Website from a Shared Environment, the Player does not receive a bonus.

13.2 If there is more than one Player Account from the same IP address, all the Player's bonuses and winnings may be canceled.

13.3 Only one type of bonus is eligible for a deposit.

13.4 Bonuses exceeding the amount of EUR/USD 2.000 will only be granted after the Player has passed the Verification Checks as described in art. 6.

14 CHAT FACILITY

The Company may provide the Player with a chat facility to enable the Player to communicate with the Customer Support Team. The Company may review and keep a record of all such content on the Company's chat facility.

15 RESPONSIBLE GAMBLING: PLAYER PROTECTION AND CONTROLS

15.1 For Players who want to restrict themselves, the following tools/options for limits and self-exclusion are available:

- Set a limit on the amount the Player can deposit into the Player Account within a specified period of time.
- Set a limit on the amount the Player can wager within a specified period of time.
- Set a limit on the losses the Player can incur within a specified period of time.
- Set a limit on the amount of time the Player can play in any one session.
- Self-exclude the Player from playing. In setting any cooling off period the Player has the right to suspend his/her Player Account for a period of no less than seventy-two (72) hours.

Deregistration from the Website

15.2 To implement the tools/options for limits and self-exclusion referred to in article 15.1, a request should be sent to the Customer Support Team, as per the Responsible Gaming Policy

15.3 The consequences of the limits referred to in article 15.1 is that the Company will make all reasonable efforts to not accept a wager from the Player contrary to a limit or exclusion set by Player. However, the Company does not accept any responsibility if the Player's use of the Website to place bets is not detected or noticed by the Company.

15.4 The Company is committed to supporting Responsible Gaming initiatives and recommends the Player to visit organizations dealing with problematic gambling in the Player's country of residence.

15.5 If the Player breaches the Company's Responsible Gambling Policy, the Company may suspend or close the Player's Player Account.

16 CLOSING THE PLAYER ACCOUNT

16.1 The Player may close his/her Player Account at any time by contacting Customer Support.

16.2 The Company reserves the right to close a Player Account at any time for any reason. If the Company terminates a Player Account for any reason the provisions set out below shall apply:

(i) the Player agrees that the Company shall not be liable to the Player for any termination of his/her Player Account or the Player's use of the Website; (ii) the Player's sole remedy in the event of termination of the Player's Player Account shall be the re-imbursement of any undisputed Player Account balance the Player may then have, in accordance with the payments limitations as set in article 9.23; the Company shall have no further liability to the Player whatsoever. (iii) where the Company terminates a Player Account due to the Player breaching any of these Terms, the Company has the unfettered discretion to void any winnings and confiscate any balance. Such breaches include, but are not limited to:

- if the Player has more than one active Player Account (or controls more than one active Player Account);
- if the Player is in breach of any of the Player's warranties;
- if the Player has opened a Player Account having previously been banned from opening any further Player Accounts on the Website;
- if the Company is required to do so pursuant to any legal and regulatory obligations;
- if the name on the Player Account does not match the name on the payment method used to make deposits;
- if the Player provides incorrect or misleading registration information;
- if the Player resides in a Restricted Jurisdiction;
- if the Player has allowed or permitted (intentionally or unintentionally)

someone else to play on his/her Player Account; • if the Player has "charged back" any of the deposits made with his/her credit card on the Player Account; • if the Player is found colluding, cheating, money laundering or undertaking fraudulent activity; • if it is determined by the Company that the Player has employed or made use of a system (including machines, computers, software or other automated systems) designed specifically to defeat the casino; • if the Player makes statements that are sexually explicit or offensive in the chat facility or to any of the Company's staff members, including expressions of bigotry, racism, hatred or profanity; • the use of robotic, mechanical, electronic, or other devices to automatically make playing decisions in any game (without the Company's explicit consent); or • if the Company should become aware that the Player has played at any other online casino in bad faith or under any of the circumstances set out above.

16.3 Upon termination of his/her Player Account, the Player agrees and acknowledges that his/her rights to use the Website shall immediately terminate and the Player will remove any Software provided to the Player or downloaded from the Website.

17 INACTIVE ACCOUNTS

If the Player does not use his/her Player Account to carry out any betting activity for a period of 3 consecutive months, such Player Account shall be deemed to be inactive. Any inactive Player Account will be subject to the following:

- Following 3 months of uninterrupted inactivity, the Company will send a reminder mail to the Player via the e-mail address saved in the Player Account details. Upon receipt of this reminder mail, the Player will have 30 days to log into the Player Account. If no login is registered within this 30-day period, EUR/USD 5 of real money credit will be deducted from the balance. If the balance is less than EUR/USD 1 then the whole amount will be deducted. If the Player Account remains inactive for 6 consecutive months since the last login, the Player will be sent a reminder mail every month and a monthly charge of EUR/USD 5 will be incurred and deducted from the real money Player Account accordingly until either the balance is EUR/USD 0 or the Player log into the Player Account.
- The Company reserves the right to close any inactive Player Account whose balance has been reduced to zero for a consecutive period of 3 months. Before re-opening an inactive account, the Company has the right to request additional information and documents from the Player to establish that the Player Account has not or is not being misused by the Player in any manner possible.

18 DOWNLOADS

For certain of the Company's betting products and Services offered through the Website the Player may need to download Software to use them and the Company will license such Software to the Player (or sublicense to the Player, to the extent such Software is owned by a third party). The terms upon which the Player may download and use any such Software will be made available to the Player at the time of download and must be accepted by the Player prior to his/her use of that Software.

19 INDEMNITY

The Player agrees to fully indemnify, defend and holds the Company, its officers, directors, employees, agents, and suppliers, harmless immediately on demand, from and against all claims, liabilities, damages, losses, costs and expenses including legal fees, arising out of any breach of

the Terms by the Player or any other liabilities arising out of the Player's access and use of the Website and Games or the Software on the Website (or by anyone else using the Player's username and password).

20 FRAUD

20.1 The Company reserves the right to seek criminal and contractual sanctions against the Player if the Player is involved in fraud, dishonest or criminal acts and will make such reports as necessary to the authorities.

20.2 The Company reserves the right to withhold payment to the Player where the Player are suspected of engaging in fraudulent, dishonest or criminal activities.

20.3 The Player shall indemnify and shall be liable to pay the Company, on demand, all costs, charges or losses sustained or incurred by the Company (including any direct, indirect or consequential losses, loss of profit and loss of reputation) arising directly or indirectly from the Player's fraud, dishonesty or criminal actions.

20.4 The following activities are amongst others prohibited on the Website:

a)

Collusion: covert co-operation between participants of a game, including chip dumping and transfer, discussing a hand during play, multiple persons using a single Player Account and soft playing.

b)

Arbitrage betting and the use of betting strategies such as martingale.

c)

Using an advantage or influence to create injustice (commonly cheating), exploiting a potential bug, exploiting Software vulnerabilities or bugs, using automated players (also called 'bots').

d)

Using credit or debit cards seized, stolen, copied by fraudulent method, being involved in or being a part of money laundering or similar illegal acts.

20.5 Necessary steps are taken by the Company to prevent and detect these activities and to identify related players. The Company is not responsible for the damages and losses that the Player may suffer from collusion, cheating, fraud and illegal activities. The actions to be taken are at the discretion of the Company.

20.6 If a Player has suspicions someone is engaging in collusion, cheating, fraud or illegal activities, the Player must notify the Company by email.

20.7 The Company reserves the right to share the Player's identity information with the authorities, other betting sites and operators, online service provider and banks, credit card companies, electronic payment system providers and other financial institutions because of any suspected illegal or inappropriate activity and the Company will cooperate in investigating such activities.

21 COMPLAINTS AND DISPUTES AND ALTERNATIVE DISPUTE RESOLUTION

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.

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

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

21.3 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

21.4 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

21.5 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).

21.6 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.

21.7 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.

21.8 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.

21.9 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.

21.10 The Player may not commence any court proceedings 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 refrained from participation provided that the right to issue proceedings is not prejudiced by a delay.

21.11 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.

22 COMPLIANCE WITH LAWS

Any products accessed through the Website may be used only for lawful purposes and in a lawful manner. The Player agrees to comply with all applicable laws, statutes and regulations regarding the Website and any bets placed through the Website.

23 INFORMATION THE COMPANY COLLECTS ABOUT THE PLAYER

23.1 The Company processes information about the Player in accordance with its Privacy Policy. The Privacy Policy contains details on the types of information the Company collects and what the Company does with that information.

23.2 The Company is entitled to share the information the Company holds on the Player which includes personal data and betting history with the regulator and other bodies, including the police, in order to investigate fraud and money laundering and to comply with the Company's regulatory duties.

24 PROMOTIONS

Please see the Company's Standard Promotional Terms and Conditions and Significant Terms and Conditions (where applicable) for information on promotions, bonuses and offers.

25 NO WARRANTY

25.1 The Company will endeavor to provide the Website using the Company's reasonable skill and care. The Company makes no further warranty or representation, whether express or implied, in relation to the Website. All implied warranties or conditions of satisfactory quality, fitness for purpose, completeness or accuracy are hereby excluded to the fullest extent permitted by law.

25.2 The Company makes no warranty that the Website will meet the Player's requirements or will be uninterrupted, timely, secure or error-free, that defects will be corrected, or that the Website or the server that makes it available are free of viruses or bugs or represents the full functionality, accuracy, reliability of the materials or as to results or the accuracy of any information obtained by the Player through the Website.

25.3 In the event of systems or communications errors relating to the generation of random numbers, bet settlement or other elements of the betting product, the Company will not be liable to the Player as a result of any such errors and the Company reserve the right to void all bets on the draws in question. In the event of a discrepancy between the result showing on the Player's Software and the Company's server software, the result showing on the Company's server software shall be the official and governing result.

25.4 In rare circumstances the result displayed within a game may be incorrect. In the event of a dispute, the result recorded on the game server will stand as the correct outcome. Nothing in this article shall affect the Company's rights as set out in article 27 (Right to Void).

26 RIGHT TO VOID

26.1 Where, on the Website, the Company makes an error (whether human or otherwise), the Company will be entitled to declare the transaction/wager void and withhold any payments.

26.2 The Company has the authority to adjust the Player Account to reflect the true outcome and rectify the error. An example of such an error might be where a failure occurs in one of the Company's systems or where the Company enters a result of an event incorrectly.

26.3 Players found abusing such errors/malfunctions are subject to having their Player Account closed and any deposits and/or winnings forfeited.

27 LIMITATION OF LIABILITY

27.1 The Player agrees that his/her use of the Website is at the Player's sole risk. The Company's maximum liability to the Player arising out of the Terms, whether for breach of contract, tort (including negligence), or otherwise will be limited to:

- the amount of the bet relevant to the which the liability in question has arisen;
- and • where monies paid by the Player into the Player Account have been misplaced by the Company, the return of the same amount into the Player Account.

27.2 The Company shall not be liable to the Player in contract, tort (including negligence), breach of statutory duty or otherwise arising from: business interruption (including downtime, server disruption, lagging, technical or political disturbance to game play), loss of profits (including loss of or failure to receive anticipated winnings), revenue, business, data, opportunity, business information or goodwill; or indirect or consequential loss, arising out of, or in relation to, these Terms, even if such losses are foreseeable or if the Company has been notified by the Player of the possibility of such losses.

27.3 The Company will not be responsible or liable to the Player for any loss of content or material uploaded or transmitted through the Website and the Player confirm that the Company shall not be liable to the Player or any third party for any modification to, suspension of or discontinuance of the Website.

27.4 The Company will not be liable for any breach of the Terms if it is caused by a matter beyond the Company's reasonable control, including acts of God, internet failures (including the Player's internet provider), computer equipment failures, telecommunication equipment or other equipment failures, electrical power failures, fire, lightning, explosion, war, flood, industrial disputes, sabotage, severe weather, or acts of local or central Government or other competent authorities.

27.5 Nothing in the Terms shall exclude or limit the Company's liability for death or personal injury resulting from the Company's negligence or any liability to the extent the same may not be excluded or limited as a matter of law.

28 IT FAILURE

28.1 The Company cannot be held responsible for a bet not being placed or an offer not being matched for any reason, or the Player being disconnected from the Website, including but not limited to computer malfunctions and failure of telecommunications services or internet connections.

28.2 The balance of the Player Account will always be as is recorded on the Company's server. The balance on the server when logging on to the Website, after the Player have been disconnected, will reflect the balance after completion of the last bet prior to the disconnection. This is necessary to avoid any further complications. By placing any further bets or offers on the Website, the Player accept the results of any previous bet. As such (at the Company's discretion) the results of the previous bet are no longer in dispute and no refund or other adjustments will be granted. If the Player feels the result of any of the Games is unfair or incorrect, the Player should contact the Company immediately and report the incident.

28.3 In the event of a malfunction in a Game, the Service, the Website or any of the related systems, or due to any other error, all bets placed during such period are void and will be refunded. Funds obtained from a malfunction shall be considered void, as well as any subsequent game rounds said funds, regardless of what games are played using such funds. If the Player is,

as a result of such malfunction or error, credited with funds resulting in any overpayment or over-crediting to his/her Player Account, it is the Player's responsibility to promptly inform the Company. Without derogating from such responsibility and regardless of whether the Player do notify the Company, the Player hereby agree and expressly authorize the Company upon becoming aware of any erroneous crediting, or payment of funds, to adjust his/her Player Account to recover any such funds.

29 LINKS TO THE WEBSITE

29.1 Where the Website contains links to other websites and resources provided by third parties, these links are provided for the Player's information only. The Company has no control over the contents of these sites or resources and accept no responsibility for them or for any loss or damage that may arise from the Player's use of them or their use of any information they may acquire about the Player (including personal data).

29.2 A link from the Website does not constitute an endorsement by the Company of the use of that link, the company or organization behind that link or the contents of the website reached using that link.

30 INTELLECTUAL PROPERTY RIGHTS

30.1 The Website Material is the Company's exclusive property or are used under license by the Company. The Company takes breaches of the Company's intellectual property rights seriously and may take legal action in respect of any infringements.

30.2 The names of the Company's products and Services (including, but not limited to, the names of the Games) are the trademarks of the Company or its licensors. The Website Material is protected by copyright laws and treaties around the world. All rights in and to the Website Material (including all intellectual property rights) are reserved.

30.3 These intellectual property rights include, without limitation, copyright, trademarks, the underlying software, the design, graphics, layout, look and feel and structure of the Website, database rights, design rights, domain names and rights to goodwill and/or to sue for passing off. The Player is permitted to use this material and content only as expressly authorized by the Company.

30.4 The Website Material is made available to the Player for use on a non-professional, non-commercial entertainment basis only. Any other use (including, but not limited to, republication) of the Website Material is subject to the Company's prior written approval.

30.5 Without limiting the generality of the foregoing, the Player may not sell, assign, license, distribute, copy, modify, publicly perform or display, transmit, publish, edit, adapt, create derivative works from, or otherwise make unauthorized use of the Website Material without the Company's express prior written consent. Except as permitted by applicable law the Player must not decompile, re-engineer or disassemble the Website Material, nor attempt to interfere with its correct operation. The Player agrees not to remove, obscure, or alter any copyright, patent, trademark, or other proprietary rights notices affixed to Website Material. The Player agrees not to use any automatic or manual device to monitor any of the Company's web pages or any content therein.

30.6 The Company will not be liable to the Player for any losses nor be liable to pay the Player any winnings if the Company has reasonable cause to believe that the Player has engaged in any activity prohibited by this article.

31 TRANSFER OF RIGHTS AND DUTIES

31.1 Given the fact that a Player Account is personal to that specific Player, whereby the Player has been identified, and that also the method of payments of any winnings is connected to the

Player itself, in order to avoid possible money laundering, terrorist financing or other illegal acts, the Player may not assign, sublicense or otherwise transfer or encumber in any manner whatsoever any of his/her rights or obligations under the Terms.

31.2 In case the Player encumbers any of his/her rights under the Terms, the Player shall forfeit all his/her rights under the Terms towards the Company.

31.3 In case by law, or by decision of a court the transfer of rights and/or obligations of the Player is deemed legal, all withdrawals shall be done through the same payment method and payment details chosen by the Player when placing a deposit, to ensure compliance with AML policies and regulation.

32 LANGUAGE

The Terms are written in English, and any interpretation of them will be based on the English version. The English version will always prevail if the Terms or other related documents are translated into any other language.

33 GOVERNING LAW AND CHOICE OF FORUM

33.1 These Terms shall be governed by and interpreted in accordance with the laws of Curaçao.

33.2 The Player irrevocably submits to the exclusive jurisdiction of the courts of Curaçao in relation to any disputes (including claims for set off and counterclaims) in relation to these Terms.