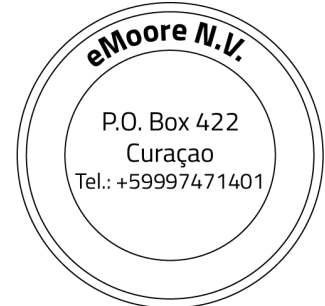


OPERATIONAL MANUAL

FITZGERALD INDUSTRIES GROUP N.V.

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



Version: 1.0

Effective Date: 29/06/2026

Prepared By: internal Compliance Department

Approved By: Director, eMoore N.V., acting in its capacity as duly appointed executive director of Fitzgerald Industries Group 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 Fitzgerald Industries Group 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

Fitzgerald Industries Group N.V.

Registration number: 124213

Registered Address: Groot Kwartierweg 10, Livestrong Building, Curaçao

Websites URLs: www.tropeziapalace.com / www.chericasino.com

2.2 Shareholding structure and infrastructure

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

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

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

In addition to corporate records, the License Holder maintains 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 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 brands (Tropezia Palace and Cheri Casino) share an identical games offering, delivered through the Alea Play aggregator. The figures below reflect the live production environment as of 2026-06-26: 6,118 games offered, supplied by 46 active software providers, with a published RTP for 100% of them. (Basis: games that are active on the casino and whose software is enabled at the gateway.)

Casino Games

- **Slots:** Digital reel-based games where players spin to match symbols and win prizes based on predefined paylines or bonus features. Slots represent the large majority of the offering (≈5,971 games).
- **Roulette:** A wheel-based game where players wager on where a ball will land, including numbers, colours, 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 player hand, the banker hand, or a tie.
- **Casino Poker:** House-banked poker variants (e.g. Casino Hold'em, Three Card Poker) where players compete against the house rather than against other players.
- **Video Poker:** Single-player draw-poker games played against a fixed payable.
- **Live Casino Games:** Real-time casino games streamed from studios with live dealers (Evolution, Playtech, Amusnet), featuring interactive gameplay.

Additional Gambling Products

- **Bingo:** 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 (e.g. Aviator, Plinko).
- **Instant Win Games:** Fast-play games where results are determined immediately, including scratch cards and digital instant-win titles.
- **Jackpot Games:** Slots featuring progressive or fixed jackpots that accumulate until won.

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 are published on the game (info folder) and all games have a freely available demo. All of them are available in multiple languages including English.

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

- The applicable minimum and maximum bet 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 ensures 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 implements and maintains 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 are 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 ensures that all betting limits are clearly defined within the relevant game configurations and are consistently applied across all channels and platforms.

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

Any changes to betting limits are 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 are 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 are 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 are 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 maintains 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 are suspended where necessary to protect players and maintain fairness.

The License Holder establishes and maintains robust audit and compliance frameworks to ensure adherence to all applicable legal and regulatory obligations.

This includes 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 are implemented to periodically assess the effectiveness of controls governing game integrity, payout accuracy, and system security.

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

The License Holder provides 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 are promptly reported to the relevant regulatory authority in accordance with applicable reporting timelines.

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

3.5 Software Providers

The License Holder uses Alea Play as a game aggregator, they provide all of the License Holder's games in only one integration.

The License Holder maintains comprehensive, accurate, and current records in respect of Alea Play and their products, including but not limited to:

- The legal name, registration details, and corporate structure;
- The jurisdictions in which the provider is licensed, regulated, or otherwise authorized to conduct gaming-related activities;
- 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 are maintained in a secure, structured, and auditable manner to ensure full traceability of the software deployment and changes throughout the system lifecycle.

The License Holder ensures that:

- Any 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, 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 are 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 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;
- Algorithmic settlement engines, applying predefined rules and logic to ensure consistent, accurate, and auditable bet settlement processes.

Manual intervention is not permitted in the determination, manipulation, or alteration of game outcomes. All outcome processes are fully automated and governed by certified systems and approved game logic.

The License Holder implements and maintains 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 are 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 are 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 offers and accepts a range of payment methods, subject to regulatory approval and applicable legal requirements, including credit and debit cards, bank transfers, electronic wallets, and other approved methods. All payment methods are provided through authorized and reputable payment service providers and integrated securely. An overview is provided in **Appendix D**.

4.2 Deposit Procedures

Deposits are only 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 are monitored in accordance with the AML Policy of the License Holder.

4.3 Withdrawal Procedures

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

4.4 Segregation and Safeguarding of Player Funds

Player funds are administratively segregated from operational funds. Daily reconciliations are performed to verify balances and identify discrepancies. Records are 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

The License Holder platform is composed of the core components below. Each component listed in the licensing framework maps to a concrete system within the License Holder ecosystem. The two casino brands (Tropezia Palace and Cheri Casino) run on the same platform and apply the same controls (AML, checks, support and responsible gaming), so the descriptions below apply identically to both.

Front-End Player Interface. The player-facing interface is delivered by two casino front-ends, Tropezia Palace and Cheri Casino. Both run on Symfony (PHP 8.3), served behind Apache and fronted by the Cloudflare CDN and WAF edge (the Cloudflare WAF is enabled on the tropeziapalace.com and chericasino.com zones, and DDoS protection is active on all production zones). Game clients are presented to the player as a provider-served iframe whose URL is generated by the aggregator (AleaPlay); the player's browser communicates directly with the provider's game server while the casino front-end embeds the launcher. The two front-ends are hosted on dedicated AWS EC2 instances.

Wallet System. The platform operates a seamless-wallet integration model: the casino holds the authoritative player balance and only debits or credits it in response to operations received from the aggregator. Deposits and withdrawals are processed through a centralised payment gateway shared by both casinos, which routes each request to the configured payment service providers and returns the outcome to the casino balance through a server-to-server callback. Every balance movement (bet, win, deposit, withdrawal and bonus) is written as a transaction record in the casino database, which supports audit and reconciliation.

Bonus Engine. Bonus and promotional logic is operated within the casino back-end and the back-office.

Risk Engine. Risk is managed by automated fraud and suspicious-activity rules and by manual review from the support team, applied at each stage of the player lifecycle (registration, deposit and withdrawal). The control function combines the following systems:

AML and sanctions screening: Dilisense, a name-based screening of players against approximately 25 PEP, sanctions and watchlist sources (such as UN, EU, UK, Swiss, French and German Treasury, Interpol and World Bank lists), returning a risk level (LOW, MEDIUM or HIGH) and a stored screening record. This is name-based screening performed at KYC, not real-time transaction monitoring.

IP and device fraud scoring: IPQualityScore, scoring player IP and device for fraud and validating phone numbers, consumed by the back-office.

Withdrawal controls: a manual game-check and responsible-gaming review at withdrawal validation, flagging behavioural signals such as withdrawals cancelled within 24 hours, denied deposits, bets placed during validation, and recurrence of game-checks.

Responsible-gaming controls (deposit limits, cool-off and self-exclusion) are enforced.

BIN lookup (iinlist) supports card-origin checks during payment.

Reporting Systems. Business reporting and analytics are provided by the back-office, covering player and transaction analytics over the casino databases (including IP fraud-scoring data) as well as finance reporting (PSP acceptance statistics by payment method and card type, BIN lookup, currency and operation reporting). Infrastructure and operational reporting is provided by the monitoring stack: CheckMK for host and service state, Grafana with Loki log aggregation (logs shipped by Grafana Alloy), and CloudWatch for AWS WAF logs.

Administrative Backend. The administrative back-end is the tools platform, the central operations hub for the estate. It provides back-office administration, player and transaction analytics, KYC and AML screening, finance operations and PSP statistics, SMS campaigns and 2FA delivery, game and provider management (game launch, free-spins, GraphQL to AleaPlay), IP and fraud scoring, and server monitoring and command execution. Administrative access is protected by two-factor authentication and role-based access control (see Section 5.3).

Gaming Platform / Aggregator. Underpinning the wallet and front-end is the games aggregator AleaPlay, the single configured aggregator for both casinos. Game outcomes and the random number generation are determined on the provider side; the casino performs no game logic (see Sections 3.5 and 3.6).

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 implements and maintains comprehensive testing and monitoring procedures to ensure the integrity, security, and reliability of all gaming operations and supporting systems.

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

6.2 Monitoring Frequency

Monitoring Activity	Minimum Frequency
Vulnerability Scans	After major changes
Penetration Tests	At least annually
Backup Restoration Testing	Quarterly
Disaster Recovery Testing	Annually
Access Control Reviews	Quarterly
System Availability Monitoring	Continuous (24/7)
Transaction Monitoring	Continuous (24/7)
Responsible Gaming Monitoring	Continuous (24/7)

7. STORAGE OF PLAYER PERSONAL DATA

7.1 Personal Data Collected

The License Holder collects and processes the following categories of personal data. Both casino brands collect the same categories, and all categories listed in the licensing framework are applicable.

Identification data. Title or gender, username, first and last name, captured at player registration.

Contact information. Postal address (street, city, state or region, postcode, country), email address, and telephone numbers. Language and account currency preferences are recorded alongside.

Date of birth. Collected for every player as a mandatory field, used for age verification and as a KYC identity attribute.

Payment information. Payment instruments and transaction routing are processed through the the License Holder gateway and its connected payment service providers.

Transaction records. A complete record of deposits and withdrawals (amount, currency, payment method, status, source IP, timestamps) and aggregate transaction counters per player, with an operation-by-operation financial audit trail.

Gaming activity. Per-round and per-session gaming history, wager and win operations, and live player balance (real and bonus). Gaming operations originate from the AleaPlay seamless-wallet integration; game outcomes are determined by the provider.

Device and IP information. Connection IP address, user agent, and associated session and connection metadata, including the registration IP and device characteristics.

KYC documentation. Identity and verification documents uploaded by players, together with their metadata (status, document type).

AML and sanctions screening data. Name-based screening data (first name, last name, date of birth, gender) processed against PEP and sanctions sources through the Dilisense service, with the screening result (risk level and hit count) retained.

7.2 Data Storage and Security

Personal data are stored securely using appropriate technical and organizational measures.

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

Encryption is applied to:

- Data in transit
- Data at rest
- Backup storage

7.2 Data Retention

Data retention complies with applicable legal and regulatory requirements.

- Curaçao legal requirements

- AML/CFT obligations
 - Regulatory recordkeeping obligations
- Archived records remain retrievable for regulatory review.

7.4 Access Logging and Control

Administrative access to personal data is 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 strictly prohibits 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 implements 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;

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

9.2 Self-Exclusion Procedures

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

9.3 Vulnerable Player Detection

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

Monitoring mechanisms 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 is 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 implements 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 are 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, hosted on Amazon Web Services (AWS) in the eu-west-

2 region, supporting continuous operations and regulatory compliance. It comprises :

Application servers: the two casino front-ends (Tropezia Palace and Cheri Casino), the centralised payment gateway, and the back-office platform, each running on dedicated AWS EC2 instances behind Application Load Balancers.

Database servers: managed AWS RDS (Aurora MySQL) clusters, replicated across multiple Availability Zones and not reachable from the public internet.

Wallet system: player balances are held in the casino application databases under a seamless-wallet model, with deposits and withdrawals processed through the centralised payment gateway.

Security infrastructure: Cloudflare (DNS, CDN, WAF and DDoS protection) at the edge, an AWS WAF on the casino load balancers, TLS encryption in transit, data encryption at rest, role-based access control with two-factor authentication, and a corporate VPN for administrative access.

Cloud hosting: AWS (EC2, RDS, load balancers, S3, CloudWatch, SES), primarily in eu-west-2, with a corporate VPN endpoint in eu-west-3..

Monitoring systems: continuous (24/7) infrastructure and service monitoring, centralised logging and dashboards, and active checks against critical third-party services.

Backup systems: periodic backups of databases and servers on AWS (daily full plus incremental backups), with multi-Availability-Zone redundancy. Backup and disaster-recovery arrangements are detailed in Section 10.4.

The gaming platform is provided by a single external game aggregator (AleaPlay) under a seamless-wallet integration, in which game outcomes and the random number generation are determined on the provider side. A detailed infrastructure inventory is maintained internally and is available to the regulator on request.

10.2 Business Continuity Plan (BCP)

The License Holder maintains a Business Continuity Plan addressing the key disruption scenarios that could affect its operations: cybersecurity incidents, data corruption, hosting outages, payment interruptions, and system failures. For each scenario the plan defines the detection, response and recovery measures and the roles responsible for coordinating the response. The BCP is reviewed periodically and approved by senior management.

● Scenario	● Detection	● Response	● Recovery
● Cybersecurity incident	● Continuous monitoring and alerts	● Incident process (Section 16.3); containment; senior management and Compliance informed	● Restore affected systems from backups ; verify integrity before return to service
● Data corruption	● Monitoring and data-integrity checks	● Isolate the affected system; invoke the incident process	● Restore from backups (daily plus incremental); validate data
● Hosting outage	● Infrastructure monitoring	● Use multi-Availability-Zone redundancy; escalate to the cloud provider	● Restore service; confirm health through monitoring
● Payment interruption	● Monitoring of payment-	● Route transactions to an alternative payment provider; inform support	● Resume normal processing once the provider is restored

provider availability			
• System failure	• Monitoring and alerts	• Incident process; manual remediation by the technical team	• Restore from backups or redeploy; confirm through monitoring

10.3 Disaster Recovery

The License Holder's disaster-recovery arrangements protect against data loss and service disruption:

Automated backups: databases and the servers holding data are backed up periodically on AWS (daily full plus incremental backups), enabling records to be restored in the event of data loss.

Redundancy: front-end traffic is distributed across multiple Availability Zones by the load balancers, and the database storage is replicated across multiple Availability Zones.

Failover and recovery: services and data can be recovered from backups, with integrity verified before return to service.

Recovery testing: backup restoration and disaster-recovery procedures are tested periodically (see the monitoring frequencies in Section 6.2).

11. RESPONSIBLE GAMING IMPLEMENTATION

11.1 Responsible Gaming Policy

The License Holder establishes, implements, and maintains 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 is maintained and made available in a manner that ensures transparency, accessibility, and compliance with applicable regulatory requirements.

The Terms and Conditions:

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

The Terms and Conditions include, at a minimum, 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 establishes and maintains 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 are 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 are handled in a structured, transparent, and consistent manner, in accordance with the procedures defined in the Player Complaint Policy.

Upon receipt, each complaint is:

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 ensures 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 has the right to escalate the matter in accordance with the escalation procedures outlined in the Player Complaint Policy.

Escalation options 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:

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

13.4 Recordkeeping

The License Holder maintains 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:

- are securely stored in digital form within the License Holder’s systems;
- contain sufficient detail to demonstrate the full lifecycle of each complaint; and
- are 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 are 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 maintains 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 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 are 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 implements technical and organisational measures to ensure the security, integrity and confidentiality of all records. These measures include:

Encryption. Data is encrypted both in transit (TLS) and at rest. Databases and storage volumes are encrypted, protecting records against unauthorised access.

Backup procedures. Databases and the servers holding data are backed up periodically on AWS, with daily full backups complemented by incremental backups. This ensures the regular and secure replication of critical data and the ability to restore records in the event of data loss.

Immutable logging. Logging mechanisms are in place to prevent the unauthorised alteration or deletion of critical records.

Access controls. Role-based and IP-based access control restricts records to authorised personnel on a need-to-know basis.

The License Holder also operates monitoring mechanisms to detect unauthorised access, data breaches and irregular activity involving maintained records.

14.3 Audit Trails

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

- 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 and closure;
Security-related events, including access attempts, system alerts and detected incidents.

All audit trail records are securely stored and protected against unauthorised modification or deletion, include sufficient detail to reconstruct events and support investigations, and are retained for a period consistent with applicable regulatory, audit and legal requirements.

Audit trails are regularly reviewed and are available for internal audits, external audits and regulatory inspections.

15. AML/CFT COMPLIANCE

15.1 AML Framework

The License Holder establishes, implements, and maintains 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 is designed to prevent, detect, and report money laundering, terrorist financing, and other forms of financial crime. It includes 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 applies 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 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 are 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 implements automated transaction monitoring systems to identify and assess potentially suspicious activity in real time and on a retrospective basis.

Monitoring systems are 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 are 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 ensures that such matters are promptly escalated to the MLRO for assessment and determination.

Where required by applicable laws and regulations:

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

The License Holder maintains 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 identifies, classifies, and manages all incidents that may impact operations, system integrity, player protection, or regulatory compliance.

Incidents 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 operates a structured eight-stage incident lifecycle to ensure consistent handling, timely resolution and regulatory compliance. Each stage is supported by the operation's monitoring, alerting and ticketing systems (CheckMK, Grafana with Loki). Incidents are escalated according to their severity, with a designated Incident Manager and senior-management involvement for major incidents.

1. Identification (Detection). Incidents are detected through several channels operating continuously (24/7):

Infrastructure monitoring: CheckMK monitors the production hosts and services, including active checks against critical third parties (the gaming aggregator AleaPlay; the payment service providers; the SMS, fraud and KYC providers).

Logging and dashboards: Grafana with Loki

log aggregation provides operational dashboards, including a traffic-light infrastructure health view and casino, payment and security dashboards.

Alerting: monitoring alerts are delivered by email and SMS. Game-availability incidents are raised by a dedicated game-load monitor that emits per-incident alerts and writes structured events to the log platform.

Support reports: operational and player-facing issues are also surfaced by the support team.

2. Categorization. Incidents are classified by nature (technical, security, operational or compliance) and by criticality. Monitoring rules encode a criticality distinction at the detection layer, with tighter thresholds for critical third parties than for standard checks.

3. Diagnosis. Root-cause investigation relies on the centralised observability stack (service status, dashboards and log queries) supplemented by controlled server access. A library of reusable operational command groups supports diagnosis and remediation.

4. Escalation. Incidents

are escalated according to their severity and potential impact. Operational incidents are escalated to the technical (development) team, and player-facing issues through the support lead. Major or high-risk incidents trigger an enhanced response: a designated Incident Manager coordinates the response, senior management

(including the Managing Director) is informed, and the Compliance function is involved where an incident has regulatory implications.

5. Resolution. Remediation is performed by the technical team, combining AWS console operations and controlled server intervention. Any action carrying production impact requires explicit confirmation before execution.

6. Recovery. Service restoration is confirmed through the same monitoring channels used for detection: services returning to a healthy state, dashboards confirming normal traffic and error levels, and, for game availability, an explicit recovery alert.

7. Closure. Incidents and follow-up actions are tracked, with projects organised by product (Tropezia Palace, Cheri Casino and payment gateway). Significant incidents are documented in a post-mortem write-up.

8. Continuous Improvement. Recommendations from incident post-mortems feed back into infrastructure and process improvements

16.4 LOK-Aligned Incident Reporting and Escalation Thresholds

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

16.4.1 Reportable Incidents

An incident is 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 ensures 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 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 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 maintains 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 are retained in accordance with applicable recordkeeping requirements and shall be made available to the CGA upon request.

16.5 Continuous Improvement

Incident data is analyzed on an ongoing basis to:

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

17. APPENDICES

Appendix A – Infrastructure Diagram

Appendix B – Overview Games of Chance

Appendix C – Third-Party Provider overview

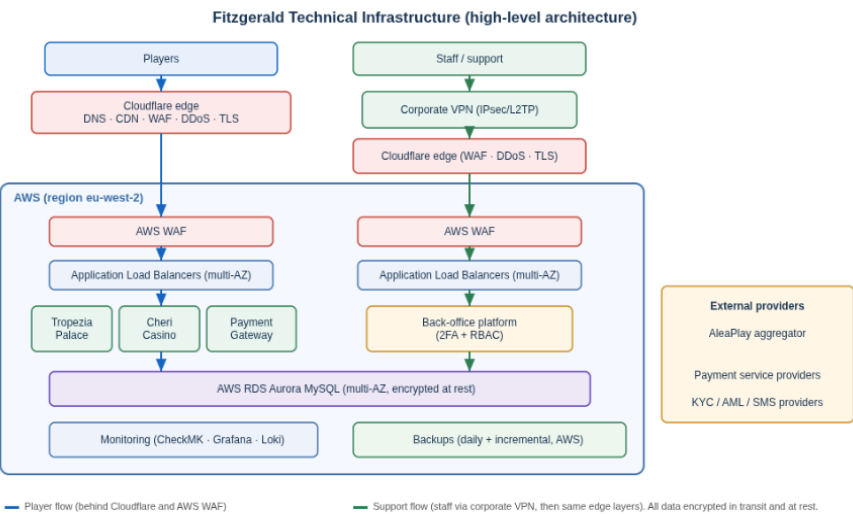
Appendix D – Overview payment methods

Appendix E – RG Notices

Appendix F – Technical measures preventing access by vulnerable persons

Appendix G –Terms and Conditions

Appendix A: Infrastructure Diagram



Appendix B – Overview Games of Chance

See separate Excell sheet

Appendix C – Third Party Provider Overview

Provider	License	Product Supplied	Software Supplied
Alea Play	OGL/2024/1280/0498	B2B Aggregator	4ThePlayer
			Amatic
			Apollo Games
			Avatarux
			BetSoft
			BetSolutions
			Big Time Gaming
			Booming Games
			Booongo
			EGT
			EGT Digital
			ELA Games
			ELK
			Eurasian Gaming
			Evolution Gaming
			Eyecon
			Fantasma Games
			Felix Gaming
			Fugaso
			Hacksaw Gaming
			Kalamba Games
			Lagio Gaming
			Maxwing Gaming
			Netent
			NoLimit City
			Novomatic
			Octoplay
			Pocket Games Soft
			Playn'Go
			Playson
			Playtech
			Pragmatic Play
			Print
			Pusch Gaming
			Quickspin
			Relax Gaming
			Ruby Play
			Skywing Group
			Spinomenal
			Spinthon
			Spride
			Stakelogic
			TaDa Gaming
			Wazdan
			Yggdrasil

Appendix D – Overview payment methods

Payment Method	Additional Info	Currency Accepted
Visa	Credit / Debit Card	EUR
Mastercard	Credit / Debit Card	EUR
Bank Transfer	Bank Transfer	EUR
Digital Wallet	Digital Wallet	EUR
Voucher	Prepaid cash-voucher	EUR

Appendix E – RG Notices

About us - Security and privacy - Terms and conditions - Responsible gaming

Account Verification - Self-Exclusion - Dispute Resolution - Anti-Money Laundering Policy - Fairness & RNG Testing Methods - Account, Pay-outs and Bonuses

Copyright 2010 - 2026 TropeziaPalace.com. All rights reserved

GCB

cert.gcb.cw

Tropezia Palace is operated under the license of Fitzgerald Industries Group N.V., a company incorporated under the laws of Curaçao with Company Number 124213 and licensed by the Curaçao Gaming Authority to offer games of chance under license number OGL/2024/941/0391

Fitzgerald Solutions Ltd with registration number HE401608, a company incorporated under the laws of Cyprus with registered office located at Archbishop Makarios III, 84, office 1, 6017, Larnaca, Cyprus established an agreement with Fitzgerald Industries Group N.V. to serve as an appointed independent representative.

18+

SPAM

FISH GAMING

QUICK SPIN

SLING SHOTS

GAMING

GROUP

SPINSTRATEGY

SPRIBE

STAKELOGIC
THINK BIGGER

TaDa
GAMING

WAZDAN

YGGDRASIL

ABOUT US - PROMOTIONS - FAQ - ACCOUNT VERIFICATION - RESPONSIBLE GAMING - TERMS AND CONDITIONS - SECURITY AND PRIVACY - CONTACT - AFFILIATES

SELF EXCLUSION - DISPUTE RESOLUTION - ANTI-MONEY LAUNDERING POLICY - FAIRNESS & RNG TESTING METHODS - ACCOUNT, PAYOUTS AND BONUSES

Cheri casino is operated under the license of Fitzgerald Industries Group N.V., a company incorporated under the laws of Curaçao with Company Number 124213 and licensed by the Curaçao Gaming Authority to offer games of chance under license number OGL/2024/941/0391

The payments services to cardholders are provided by Fitzgerald Solutions Ltd with registration number HE401608, a company incorporated under the laws of Cyprus with registered office located at Archbishop Makarios III, 84, office 1, 6017, Larnaca, Cyprus established an agreement with Fitzgerald Industries Group N.V. to serve as an appointed independent representative.

Copyright 2026 www.chericasino.com - All rights reserved

*the bonus is 100% up to 100€

SPAM

18+

GCB

cert.gcb.cw

LATEST GAMES - ABOUT US - BONDS - BANKING - NEWS - FAQ - WINNERS

Username

Password

LOG IN

Remember me

Forgot your password?

REGISTRATION

We are sorry to inform you that Tropezia Palace doesn't accept players from your country.

18+

Age Restriction Notice

Access to this platform is restricted to individuals who are 18 years of age or older.

By continuing with the registration process, you confirm that:

You are at least 18 years old.

You understand that providing false information may lead to account suspension.

Continue

Exit

CONTACT US

How can we help?

Please contact us every day from 11am to 11pm (GMT)

Live Support

WINNERS

220.000

Winnings: 1.5

Account: 1000000000

235.500

Winnings: 1.5

Account: 1000000000

1176.776

Winnings: 1.5

Account: 1000000000

817.734

Winnings: 1.5

Account: 1000000000

280.000

Winnings: 1.5

Account: 1000000000

1176.504

Winnings: 1.5

Account: 1000000000

200.000

Winnings: 1.5

Account: 1000000000

347.504

Winnings: 1.5

Account: 1000000000

1680.000

Winnings: 1.5

Account: 1000000000

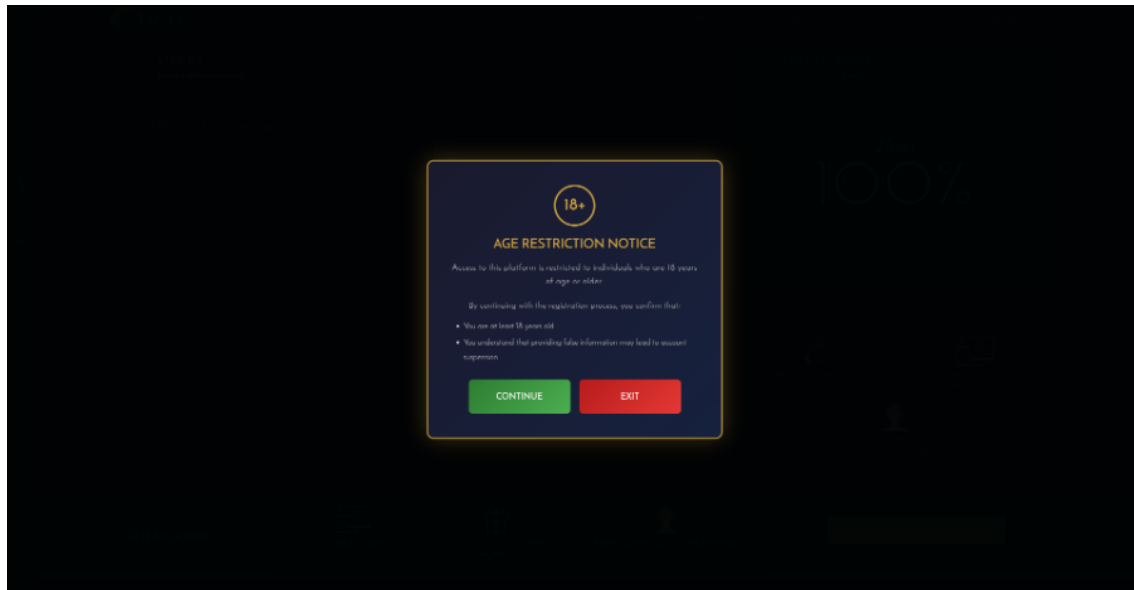
135.504

Winnings: 1.5

Account: 1000000000

We use cookies to ensure you get the best experience on our website. Learn more

OK



<https://www.chericasino.com/en/responsible.html>

<https://www.tropeziapalace.com/responsible-gaming.html?lang=en>

<https://www.tropeziapalace.com/self-exclusion.html?lang=en>

<https://www.chericasino.com/en/self-exclusion.html>

Appendix F – Technical measures preventing access by vulnerable persons

This appendix describes the technical and procedural measures in place across both casino brands (Tropezia Palace and Cheri Casino) to prevent access to gaming services by underage, self-excluded or otherwise vulnerable persons.

The two brands apply the same measures.

F.1 Age and identity verification at registration

- A valid date of birth is mandatory at registration. The registration process automatically rejects any applicant below the legal minimum age of 18, so an account cannot be created by a minor.
- Player identity, including age, is verified against uploaded identity documents through the KYC verification workflow.
- Players are screened against PEP, sanctions and watchlist sources through the Dilisense service, which returns a risk level (LOW, MEDIUM or HIGH) and a retained screening record.

F.2 Self-exclusion, cooling-off and player limits

Both casinos provide responsible-gaming tools that can be applied to a player account, by the player or by an operator:

- Deposit limits: caps on the amount a player can deposit.
- Cooling-off: a temporary break from gaming activity.
- Self-exclusion: exclusion from the service, available as a temporary or a permanent measure.

While a self-exclusion or cooling-off is active, the account is blocked from logging in, depositing, playing, and from receiving marketing communications, for the duration of the measure.

F.3 Detection of vulnerable players and intervention

Detection of at-risk behaviour combines automated, risk-based thresholds and alerts with manual review by trained staff.

- Automated monitoring applies risk-based thresholds to player activity and raises alerts on behavioural signals such as excessive or increasing deposit activity, rapid or repetitive wagering, extended or continuous gaming sessions, and repeated failed deposit attempts or unusual payment patterns.
- A structured withdrawal review (the game-check) is carried out when a withdrawal is pending validation. It examines responsible-gaming signals such as withdrawals cancelled within 24 hours, denied deposits, bets placed during validation, and repeated game-checks.

- The player's deposit, wagering and session history is available to operators to assess behaviour during the review.
- Where signals of harm are identified, the support team intervenes using the available controls (responsible-gaming messaging, account limits, cooling-off or self-exclusion) as appropriate.

Appendix G –Terms and Conditions

See separate provided Terms and Conditions for both URLs