

OPERATIONS MANUAL

Luminect Limited B.V.

a Company with registered address at KAYA RICHARD J. BEAUJON Z/N, CURACAO,
registration number 165187, CGA License number OGL/2024/358/0707 (herein after referred to
as “**Company, License Holder**”)

KEY INFORMATION

Approving Official(s): Gouloud Hammoud obo Guardian Corporation Curaçao B.V. the Statutory Director

Responsible Office: Gouloud Hammoud obo Guardian Corporation Curaçao B.V. the Statutory Director

Effective Date: 29.07.2026

Next Review Date: 29.07.2027

1. Purpose

This Operations Manual establishes the governance, operational controls, compliance framework, policies, and procedures governing the operation of Luminect Limited B.V.'s online gaming business under CGA License OGL/2024/358/0707. It incorporates operational information contained in Version 1.0 of the Operations Manual questionnaire and aligns it with CGA regulatory expectations.

2. Corporate Governance

2.1 Governance Structure

The Company maintains:

- Board of Directors
- Managing Director
- Key Compliance Functionary (KCF)
- MLRO
- Information Security Function
- Responsible Gaming Function
- Operations Team
- Customer Support Team
- Payments Team
- Third-Party Risk Management Function

The Board retains ultimate responsibility for regulatory compliance and risk management.

2.2 Three Lines of Defense

First Line

Operational management.

Second Line

- Compliance

- AML/CFT
- Responsible Gaming
- Information Security

Third Line

- Independent Audit
- External Reviews
- Regulatory Assessments

3. Gaming Operations

3.1 Games Offered

The Operator offers:

- Online Casino
- Sports Betting
- Live Casino

via approved third-party providers through the Hub88 platform.

3.2 Games Register

The Company maintains a Games Register containing:

- Game title
- Provider
- RTP
- Certification
- Jurisdictional restrictions
- Version control
- Release approval

Games cannot be deployed without documented approval.

4. Customer Onboarding & KYC

4.1 Registration Requirements

The following information is collected:

- Name
- Date of Birth
- Address
- Nationality
- Email Address
- Telephone Number

The system prevents registration of persons under 18 years of age.

4.2 Identity Verification

Verification is mandatory:

- Before first withdrawal
- At specified AML thresholds
- When suspicious activity is detected
- For high-risk customers

Required documents:

- Government-issued ID
- Proof of Address
- Payment Ownership Evidence

5. AML/CFT Program

5.1 Risk-Based Approach

Risk assessments consider:

Customer Risk

- High-value players
- PEPs
- Adverse media matches

Geographic Risk

- FATF High-Risk Jurisdictions
- FATF Grey List Jurisdictions
- Sanctioned Countries

Product Risk

- Sports Betting
- Live Casino
- Casino Products

Transaction Risk

- Rapid deposits
- Withdrawal anomalies
- Bonus abuse
- Structuring

5.2 Screening

The Operator utilizes:

- LexisNexis Compliance Lens
- PEP Screening
- Sanctions Screening
- Adverse Media Screening

Ongoing screening occurs every 24 hours.

5.3 Monitoring

The Operator uses:

- SEON
- Internal AML Monitoring Tools

Monitoring includes:

- Deposit behaviour
- Payment anomalies
- Linked accounts
- Suspicious activity indicators

6. Payment Operations

Approved Payment Methods

Current payment methods:

- Bank Cards
- Bank Transfers
- E-Wallets

PSPs:

- PaymentIQ
- Brite
- AstroPay
- PayRetailers
- Gigadat
- InPay

The Operator does not currently accept crypto-assets.

Closed-Loop Withdrawal Policy

Withdrawals must be returned to the original funding source where possible.

Third-party payments are prohibited.

7. Responsible Gaming Program

Available Controls

Players can access:

- Deposit Limits
- Wager Limits
- Loss Limits
- Reality Checks
- Cooling-Off Periods
- Self-Exclusion
- Self-Assessment Tools

Vulnerable Persons

The Company identifies:

- Minors
- Self-Excluded Customers
- Problem Gamblers
- Financially Distressed Individuals

Appropriate interventions are documented and retained.

Self-Exclusion

Available periods:

- 1 Year
- 3 Years
- 5 Years
- 10 Years
- Lifetime

All associated brands are covered by exclusions.

8. Information Security

Security Controls

The Company maintains:

- MFA
- RBAC
- VPN Controls
- TLS 1.2+
- Encryption At Rest
- Security Monitoring
- Audit Logs

Vulnerability Management

- Regular patching
- Vulnerability scanning
- External penetration testing
- Security reviews

External penetration testing provider:

- Neterix

9. Vendor & Outsourcing Management

All critical suppliers undergo due diligence covering:

- Licensing
- Regulatory Standing
- Information Security
- Business Continuity
- AML Controls

Critical suppliers include:

- Hub88
- LexisNexis
- PSP Providers
- SEON

Vendor reviews occur annually and following material incidents.

10. Business Continuity & Disaster Recovery

Backup Requirements

- Daily backups
- Encrypted backups
- Geographically separate storage
- Restoration testing

Incident Recovery

The Company is as follows:

1. Identify
2. Contain
3. Investigate
4. Remediate
5. Recover
6. Document

Material incidents are reported to the CGA.

11. Complaints Management

Complaint Stages

Stage 1

Customer Support

Stage 2

Management Review

Stage 3

Compliance Review

Stage 4

ADR Referral

ADR Provider:

- EGIS-FZCO

Every complaint is:

- Logged
- Investigated
- Responded to in writing
- Retained for inspection

12. Regulatory Reporting

The KCF coordinates:

- CGA requests
- Incident reports
- Change notifications
- Key person changes
- Ownership changes
- AML reporting

Records must be provided without delay upon regulatory request.

13. Record Retention

Record Type	Retention
KYC Records	Minimum 5 Years
AML Records	Minimum 5 Years
Transaction Records	Minimum 5 Years
Responsible Gaming Records	Minimum 5 Years
Complaints Records	Minimum 3 Years
Security Logs	Regulatory Minimum

14. Annual Reviews

The following are reviewed annually:

- Operations Manual
- AML Program
- Information Security Policy
- Responsible Gaming Policy
- Risk Assessment
- Vendor Register
- Business Continuity Plan
- Incident Register

15. Board Certification

The Board certifies annually that:

- Controls are operating effectively.
- Appropriate resources are available.
- AML/CFT measures remain effective.
- Responsible gaming controls are operational.
- Regulatory obligations are continuously monitored.
- Material deficiencies are remediated promptly.

	Question	Answer
Games of Chance offered (Games Register)	1. Which games are offered to players (casino games, sports betting, live casino, lotteries, bingo, poker, fantasy sports, crash games, or another category)?	Casino Games, Sports Betting, Live Casino.
	2. For each game type, what are the basic rules of play?	The basic rules of play for each game type are defined in the game rules published within the relevant game interface and on the website, as supplied and documented by the licensed game providers. Players are able to review the applicable game rules before participating. Game-specific details are maintained in the Games Register and provider certification records.
	3. Are any games supplied by third-party providers?	Yes. Games made available on the websites are supplied by licensed or authorised third-party game providers and, where applicable, are independently tested and certified in accordance with applicable regulatory and technical standards. Providers are onboarded subject to the Operator's third-party and vendor due diligence framework, which assesses regulatory status and licensing, reputation and track record, security practices and data handling procedures.
	4. Which game providers are used?	The game providers used by the Operator are recorded in the Games Register. Game provider / aggregation provider: Hub88
	5. Are any games restricted to specific jurisdictions or player categories?	Access to games content is restricted from jurisdictions where gambling is prohibited or restricted, or where regulatory requirements cannot be satisfied, including sanctioned and high-risk jurisdictions. Players must be at least 18 years of age, or the higher legal minimum age in their jurisdiction. Individual game-level or player-category restrictions, where applied by providers or by back-office configuration, are recorded in the Games Register.

	6. How does the operator ensure that only approved or permitted games are made available?	The Operator ensures that only approved and permitted games are made available through a combination of controls: (i) an approved Games Register recording each game authorised for release; (ii) due diligence on game providers before onboarding, under the third-party and vendor due diligence framework; (iii) game certification requirements, with games supplied by licensed or authorised providers and independently tested where applicable; (iv) change approval before any game is added, amended or removed, applied through back-office configuration; (v) role-based access control, least privilege and multi-factor authentication over the back-office systems used to configure the game lobby; and (vi) periodic reconciliation of the live game lobby against the approved Games Register, with any discrepancy investigated and corrected.
Payment possibilities	7. Which deposit methods are accepted?	The Operator does not currently accept crypto-assets for deposits or withdrawals. Deposits are currently processed through fiat payment methods and authorised third-party payment service providers (PSPs). Fiat methods may include bank cards, bank transfers and e-wallets, subject to availability by location, regulatory requirements and payment provider availability. Cash deposits are not accepted, credit is not offered, and cards issued from FATF high-risk jurisdictions are blocked. The Operator has plans to implement an operator-managed crypto payment and wallet-control environment. This is not currently live. If implemented, it will be introduced only after appropriate governance, AML controls, wallet controls, transaction monitoring, reconciliation, recordkeeping, security controls and regulatory requirements have been addressed. PSP names: Payment IQ, Brite, AstroPay, PayRetailers, Gigadat, InPay.
	8. Which withdrawal methods are available?	The Operator operates a closed-loop policy: withdrawals are returned to the same payment method used to deposit wherever possible. Where this is not possible, the Operator makes all reasonable efforts to process the withdrawal directly to the player by bank transfer. The Operator does not currently accept crypto-assets for deposits or withdrawals; crypto withdrawals are not available. All withdrawals are subject to completion of identity verification, wagering requirements, and fraud, AML and compliance checks before processing.

	9. Are fiat currencies, crypto-assets, vouchers, e-wallets, bank cards, bank transfers, or alternative payment methods used?	Fiat currencies are used. Fiat payments are accepted only from accounts held with financial institutions or through authorised payment providers, and may include bank cards, bank transfers and e-wallets. The Operator does not currently accept crypto-assets for deposits or withdrawals. Cash is not accepted and the Operator does not offer credit to players. Vouchers and other alternative payment methods are not identified in the Operator's policy documentation. The Operator has plans to implement an operator-managed crypto payment and wallet-control environment; this is not currently live.
	10. Which payment service providers are involved?	Fiat payments are processed by authorised third-party payment service providers. All PSPs are subject to due diligence before onboarding and to periodic review. The Operator does not currently accept crypto-assets, and no crypto payment provider is currently engaged. PSPs: Payment IQ, Brite, AstroPay, PayRetailers, Gigadat, InPay.
	11. Are there minimum and maximum deposit and withdrawal limits?	Yes. Deposit limits may apply, and the Operator imposes minimum and maximum withdrawal limits which may vary by payment method, player verification status, risk classification, currency and operational or regulatory requirements. Applicable limits are displayed within the website, cashier or payment interface, and withdrawals exceeding operational or provider limits may be processed in instalments. Players may additionally set their own responsible gaming deposit limits on a 24-hour, 7-day or 30-day basis. The configured minimum and maximum values are maintained in the back-office/cashier configuration and displayed to players in the cashier.
	12. Are payment methods subject to verification before use?	Yes. Payment methods must be registered in the player's own name, and the Operator verifies ownership of payment methods at any time, including front/back of card copies and bank letters or statements confirming card or account ownership. Proof of identity and proof of address are requested when cumulative transactions reach NAf 4,000, in high-risk scenarios, and in all cases before the first withdrawal is processed. Withdrawals are not processed until the requested verification has been received.

	13. Are deposits and withdrawals only permitted through accounts held in the player's own name?	Yes. Deposits from accounts not held in the player's own name are not permitted, and the use of third-party payment methods is strictly prohibited. The closed-loop withdrawal policy returns funds to the original deposit method wherever possible. Where third-party payment use is identified, the account may be suspended or closed, winnings derived from the activity may be confiscated, and deposited funds returned to the original payment source where legally required, in line with the AML and Fraud Policy.
	14. How are failed, reversed, or suspicious payments handled?	Failed or rejected payments are investigated with the relevant PSP, and deposits may be rejected or reversed where payment irregularities are identified. Chargebacks and payment reversals are handled under the Terms and Conditions: the account may be suspended, balances frozen pending investigation, associated bonuses and winnings voided, amounts offset against the account balance, and repeated chargebacks may lead to permanent closure. Suspicious payments are flagged by automated monitoring (deposit anomalies, mismatched payment details, high-volume transactions) and by staff, and are escalated to the MLRO, who acknowledges internal Unusual Transaction Reports within 24 hours and completes review within 48 hours; where required, disclosures are made to the FIU Curaçao.
Bet amounts	15. What are the minimum and maximum bet amounts per game?	Minimum and maximum stakes are defined per game by the relevant game provider and recorded in the game rules and provider documentation. Game-specific details are maintained in the Games Register and provider certification records.
	16. Are limits different per game, provider, player category, or jurisdiction?	Stake limits may vary per game and provider, and maximum bet limits may also apply during bonus play in accordance with promotion-specific terms. Jurisdictional or player-category variations, where applied, are maintained in back-office configuration and the Games Register. Game- and provider-level limit details are maintained in the Games Register.
	17. Are stake limits configurable by the player?	Players cannot alter the stake ranges of individual games, which are fixed by the game provider. However, players may set their own responsible gaming wager limits (as well as deposit and loss limits) on a 24-hour, 7-day or 30-day basis through their account settings, which restrict total staking across the site.

	18. Are internal risk limits applied by the operator?	Yes. The Operator applies internal risk-based controls, including: AML thresholds (customer due diligence at NAf 4,000 cumulative transactions; MLRO risk profile review at NAf 5,000 or more in daily transactions; enhanced due diligence at NAf 200,000 lifetime deposits), withdrawal review and closed-loop controls, maximum bet limits during bonus wagering, and withdrawal limits by risk classification. Accounts may be restricted pending verification or investigation. Game-level and liability risk limit settings are maintained in the back-office configuration.
	19. Are responsible gaming limits applied to deposits, stakes, losses, or session activity?	Yes. Players may set deposit limits, wager limits and loss limits on a 24-hour, 7-day or 30-day basis. Reality checks configurable between 5 and 60 minutes address session activity, with automatic logout where a reality check is not acknowledged. Take a Break / cooling-off periods (1 day to 3 months) and self-exclusion (1 year up to 10 years, or lifetime) are also available.
	20. How are changes to betting limits approved and recorded?	Player-initiated limit changes follow the Responsible Gambling Policy: requests to decrease a limit take effect immediately, while requests to increase or remove a limit are subject to a 7-day cooling-off period, after which the player must confirm the change before it takes effect. All limit changes are logged in the back-office system as part of the responsible gaming records. Operator-level changes to game or risk limits are made through controlled back-office configuration, subject to change approval and captured in audit trails. Game-level stake configuration records are maintained in the Games Register and back-office configuration.
Payouts and	21. What payout percentages, odds, prize structures, or return-to-player rates apply?	Return-to-player rates, odds and prize structures are determined by the certified games supplied by the game providers and are documented in the game rules and provider certification records. Game-specific details are maintained in the Games Register and provider certification records.

	22. Are payout rules displayed to players before participation?	Yes. Each game is governed by its own rules, which are made available within the relevant game interface or through the website before participation. Promotion-specific terms, including wagering requirements, game contribution rates, expiry periods and any maximum withdrawal limits, are displayed on the website or within the relevant promotional materials before the player opts in. Game-specific RTP and payable display details are maintained in the Games Register and provider documentation.
	23. How are winnings credited to player accounts?	Winnings are credited automatically to the player's account balance by the gaming platform upon settlement of the game round, based on the official game and transaction records maintained by the Operator and the relevant game provider. Winnings derived from bonus funds may be restricted until wagering requirements are completed. The Operator reserves the right to correct account balances where errors or inaccuracies are identified.
	24. Are jackpot, bonus, tournament, or promotional payouts handled differently?	Yes. Bonus and promotional payouts are subject to promotion-specific terms, including wagering requirements, eligible games, contribution percentages, maximum bet limits, expiry periods and maximum withdrawal or cashout limits; winnings exceeding a promotional maximum may be voided. Jackpot and tournament payout arrangements depend on the relevant game provider's rules. Jackpot and tournament payout structures are maintained in the Games Register and the applicable promotion terms.
	25. Are there maximum payout limits?	Maximum withdrawal or cashout limits may apply to promotions, and operational withdrawal limits (which may be applied in instalments) are displayed in the website, cashier or payment interface. Game-specific maximum win values are defined by the game providers.

	26. What happens if a game, system, or payment error affects a payout?	In the event of a malfunction, error, interruption or failure affecting a game, betting transaction or related system functionality, affected bets may be declared void and any winnings derived directly from the malfunction may be voided, in accordance with the Terms and Conditions. The Operator may suspend affected games, correct account balances, and cancel affected transactions to restore the integrity of the services. Such events are handled as incidents under the Information Security Policy: identified, contained, investigated, remediated, recovered and documented in the Incident Log, with notification to the CGA where required (typically within 72 hours for material incidents). Payment errors are reconciled against PSP settlement records and corrected with a documented audit trail.
	27. How are disputed payouts investigated?	Disputed payouts are handled under the complaints process. The investigation reviews game logs, transaction records, the applicable game rules, provider records, settlement data and any relevant technical evidence; official game records, transaction logs and system records maintained by the Operator and/or the relevant game provider prevail in the event of discrepancy. The player receives a written, reasoned final decision, and unresolved disputes may be escalated to the independent ADR provider free of charge. Complaint records, including evidence relied upon, are retained in the complaint register.
Software used in the operation	28. What platform software is used?	The operation runs on a gaming platform supplied by a third-party platform provider, delivering the game lobby, player account management, wallet/balance functionality and back-office administration. The platform provider is subject to the Operator's third-party and vendor due diligence framework and contractual security obligations. Platform provider: Hub88

	29. Which game aggregation, wallet, payment, KYC, AML, fraud monitoring, reporting, responsible gaming, CRM, and back-office systems are used?	The operation uses, in functional terms: (i) the third-party gaming platform incorporating the player account and wallet ledger and back-office; (ii) game content integrations with licensed third-party game providers; (iii) authorised PSP integrations for fiat payments (the Operator does not currently accept crypto-assets); (iv) LexisNexis Compliance Lens for PEP, sanctions and adverse media screening, with ongoing monitoring rechecked every 24 hours; (v) SEON for automated AML/fraud transaction-monitoring (vi) in-house automated AML/fraud transaction-monitoring tools flagging deposit anomalies, mismatched payment details and high-volume transactions, supported by manual review by the Compliance and Risk teams; (vii) responsible gaming tools (limits, reality checks, cooling-off, self-exclusion) delivered through the platform; (viii) customer support via email and live chat; and (ix) HireRight for employee screening.
	30. Are systems proprietary or supplied by third parties?	Core systems – the gaming platform, game content, payment processing (PSPs) and compliance screening – are supplied by third parties. The Operator does not develop or host proprietary game software and, as crypto-assets are not currently accepted, does not hold, control or operate any virtual asset wallet. The Operator retains responsibility for configuration, oversight, access control and regulatory compliance, and vendor reliance does not transfer the Operator's AML/CFT or other regulatory obligations.
	31. Who maintains and updates the software?	Third-party providers maintain and update their respective systems (platform, games, payment and screening services) under contractual arrangements requiring compliance with data protection laws, maintenance of appropriate security controls, and notification of incidents affecting Operator data. The Operator's Information Security / IT function implements and maintains internal security controls, ensures systems are regularly patched and monitored, and oversees vendor performance, with vendor risk reviewed periodically and high-risk vendors subject to enhanced oversight.

	32. How are software changes tested before release?	Production and development environments are segregated, and secure development practices are followed in accordance with the Information Security Policy. Changes are tested in non-production environments before release, and third-party providers test their own releases prior to deployment under their contractual obligations. Games are certified before being made available, and change approval applies to game lobby and configuration changes. Detailed release and acceptance-testing procedures are maintained as controlled operational documents.
	33. How are software versions documented?	Policy and document versions are controlled through revision histories and a central policy repository. Software versions and changes are documented through change records and supplier release documentation, and game versions and certificates are recorded in the Games Register.
	34. How are access rights to software systems controlled?	Access is controlled on least-privilege and role-based access control (RBAC) principles. Multi-factor authentication is required for administrative access, back-office systems and payment systems, and secure VPN is required for administrative access. Joiner/mover/leaver processes apply: access is granted on management approval, adjusted on role change, and revoked immediately (within 24 hours at most) on departure. Access reviews are conducted at least every 6 months. Privileged access is restricted to authorised personnel and subject to monitoring and logging. Vendor access must be approved, time-limited and monitored.
Outcome-determining elements	35. Are outcomes determined by random number generators, live dealer results, sports results, player decisions, algorithms, or other mechanisms?	Game outcomes are determined by certified Random Number Generator (RNG) technology or other approved game outcome mechanisms supplied by licensed third-party game providers, in accordance with applicable regulatory and technical standards. The Operator has no ability to influence or alter game outcomes.
	36. Which systems or providers determine outcomes?	Outcomes are determined within the game providers' certified systems; the platform records the results and settles player balances accordingly. Provider names and outcome systems are recorded in the Games Register.

	37. How is randomness tested and certified?	Games use certified RNG technology and are supplied by licensed or authorised third-party providers, whose games may be independently tested and certified in accordance with applicable regulatory or technical requirements. Certification evidence is obtained from providers and retained. Testing laboratory and certification details are maintained with the provider certification records in the Games Register.
	38. Are RNG certificates available?	RNG and game certification evidence is obtained from the game providers and maintained with the Games Register. Game-specific details are maintained in the Games Register and provider certification records.
	39. How are game rules, payables, odds, and outcome logic documented?	Game rules are published within each game interface and on the website; paytables, odds and outcome logic are documented by the game providers in their game rules and certification documentation. The Operator maintains the Games Register as the consolidated record of the games offered and their key parameters.
	40. How does the operator prevent manipulation of outcomes? How are incidents involving incorrect game outcomes handled?	Outcome integrity is protected by: game logic residing in the providers' certified systems, outside the Operator's control; role-based access control, least privilege, MFA and privileged-access monitoring over back-office systems; segregation of production and development environments; logging of user access, administrative actions and financial transactions with regular review; and prohibition and detection of automated tools, collusion and exploitation of software defects under the Terms and Conditions. Incidents involving incorrect game outcomes are handled under the malfunction provisions of the Terms and Conditions (affected bets and derived winnings may be voided, balances corrected) and under the Information Security incident response process: identify, contain, investigate, remediate, recover and document in the Incident Log, with CGA notification where required (typically within 72 hours for material incidents). Affected players are notified where appropriate, and official game and system records prevail in resolving discrepancies.

Periodic test methods for quality monitoring	41. Which systems are tested periodically?	Periodic testing and review covers: backups (regularly tested restorations); disaster recovery and business continuity arrangements; access rights (reviews at least every 6 months); the Information Security Risk Register (reviewed at least annually and upon significant change); the AML control framework (independent audit or internal review at least every 18 months); responsible gaming controls (monthly reviews of RG activity logs, training records and customer interactions by the Key Compliance Officer); and game certification maintained through provider records.
	42. Are RNG tests, penetration tests, vulnerability scans, game certification tests, payment tests, load tests, disaster recovery tests, responsible gaming control tests, AML control tests, or data integrity tests performed?	RNG and game certification testing is performed by the game providers and their independent testing arrangements, with evidence retained in the Games Register. Backup restoration tests and disaster recovery arrangements are tested regularly. AML control testing takes place through the independent AML review at least every 18 months, and responsible gaming control testing through monthly compliance reviews. Payment controls are tested through regular reconciliation of PSP settlement reports against the platform ledger. Systems are regularly patched, and threats and vulnerabilities are monitored by the Information Security / IT function. Penetration testing and vulnerability scanning are managed by the Information Security / IT function, with results, findings, remediation actions, owners and verification outcomes recorded in internal security and compliance records. External penetration testing provider: Neterix
	43. How often are tests conducted?	Stated frequencies: backups at least daily, with regular restoration testing; access reviews at least every 6 months; Information Security Risk Register review at least annually and upon significant changes; independent AML review at least every 18 months; responsible gaming compliance reviews monthly; PEP/sanctions rescreening of all customers every 24 hours; policy reviews at least annually. Other testing is performed periodically in line with policy.

	44. Who performs the tests: internal staff, external auditors, labs, suppliers, or consultants?	Testing is performed by a combination of: the internal Information Security / IT function (system monitoring, patching, backup and recovery testing, access reviews); the Key Compliance Function and Key Compliance Officer (compliance monitoring, responsible gaming reviews); the MLRO (AML monitoring and risk profile reviews); independent auditors or reviewers (AML framework review at least every 18 months); Neterix (external penetration testing); and third-party game providers and their testing laboratories (game and RNG certification).
	45. How are test results documented?	Results are documented in the relevant registers and records: the Information Security Risk Register (Appendix A of the Information Security Policy), the Incident Log (Appendix B), access review records, backup and recovery test records, independent AML review reports presented to the board (and shared with the CGA where applicable), monthly responsible gaming review records, and training attendance records.
	46. How are deficiencies corrected?	Deficiencies are treated through the risk management framework: risks are mitigated through controls, accepted with documented rationale, or avoided. Identified issues are recorded in the Risk Register with owners and mitigation actions, or in the Incident Log where they arise from incidents, and remediated through the incident response process (identify, contain, investigate, remediate, recover, document). Vendor-related deficiencies are addressed through contractual obligations and enhanced oversight of high-risk vendors.
	47. Who verifies that corrective actions have been completed?	The Key Compliance Function monitors compliance with the Information Security Policy and oversees incident reporting; risk register items have named owners and are reviewed with senior management at least annually. The board of directors holds ultimate accountability, reviews and approves policies, and receives the findings of independent AML reviews. Responsible gaming remediation is verified through the Key Compliance Officer's monthly reviews, with concerns escalated to senior management and remedial actions documented.

Storage of players' personal data and other details	48. What personal data is collected from players?	In accordance with the Privacy Policy, the Operator collects: identity data (name, date of birth, gender, nationality, ID/passport number, photograph of ID, verification data); contact data (email, postal address, telephone); account data (username, hashed/encrypted password, gaming account ID, payment account details); financial data (payment method data, transaction history, deposits, withdrawals, wins/losses); gaming activity data (bets, wagers, game logs, time of play, session length, device data); technical data (IP address, device identifiers, browser/OS, cookies, geolocation where used); KYC/AML/CDD data; communications data (support correspondence, complaints, chat logs); marketing and analytics data; and self-exclusion / responsible gaming data.
	49. What identification, verification, contact, financial, gaming, technical, and communication data is stored?	All of the categories listed are stored: identification and verification records (registration details, proof of identity and proof of address documents, verification outcomes, PEP/sanctions screening results); contact details; financial records (payment methods, deposits, withdrawals, transaction history); gaming records (bets, outcomes, wins/losses, session logs); technical records (IP, device, browser data); and communications records (support and complaint correspondence, chat transcripts, records of ECDD conversations, which are retained in full).
	50. Where is the data stored? Which systems or databases contain player data?	Player data is held within the gaming platform's player account management and back-office systems, which record registration, verification, transactional, gaming and responsible gaming data, together with compliance records held by the compliance function (risk assessments, UTRs, screening results). Data is classified as Highly Confidential under the Information Security Policy and protected accordingly. Critical records platform: Hub88 (third-party PAM + aggregation), hosted on Amazon Web Services, region eu-central-1 (Frankfurt, Germany). Underlying facilities are AWS's Frankfurt availability-zone data centres (see also the Server and Data Centre section, Q130–135).

	51. Who has access to the data?	Access is restricted on a least-privilege, role-based basis to personnel who require it for their function, including customer experience/support, payments, compliance (Key Compliance Function, MLRO), responsible gaming personnel and authorised IT administrators. Vendor access must be approved, time-limited and monitored. Sensitive data must not be stored unencrypted on local devices.
	52. How is access controlled and logged?	Access control follows the Information Security Policy: role-based access control and least privilege; multi-factor authentication for administrative, back-office and payment systems; secure VPN for administrative access; joiner/mover/leaver lifecycle management with access revoked within 24 hours of departure; and access reviews at least every 6 months. Logs are maintained for user access, administrative actions and financial transactions; they are stored securely and reviewed regularly, and privileged access is monitored and logged.
	53. How is data encrypted or otherwise protected?	Data is encrypted in transit using TLS 1.2 or higher and at rest using strong encryption (e.g. AES-256). Passwords are hashed and salted and non-reversible. Backups are encrypted. Player sessions include timeout controls and protection against unauthorised access, and sensitive data must not be stored unencrypted on local devices.
	54. What retention periods apply?	Personal data is retained only as long as necessary for the purposes for which it was collected, in line with legal, regulatory and business requirements, after which it is securely deleted, anonymised or aggregated. Specific periods include: CDD/ECDD and associated AML records – minimum 5 years after the business relationship ends; complaint records – minimum 3 years; operator-initiated exclusion records – at least 5 years. Crypto-asset record retention requirements under the Crypto Asset Policy will apply only if crypto payments are implemented in future.

	55. How are data correction, deletion, or access requests handled?	Players may exercise data subject rights under the Privacy Policy, including access to and copies of their data, correction of inaccurate or incomplete data, objection to certain processing (including direct marketing), erasure subject to applicable retention obligations, restriction of processing, portability where applicable, withdrawal of consent, and complaint to a supervisory authority. Requests are made to the Data Protection Officer at dpo@spacecasino.com or dpo@xtreme.game and are responded to within 30 days. Erasure and correction are applied subject to overriding AML, regulatory and audit retention obligations.
	56. How is data protected against unauthorized access, loss, alteration, or disclosure?	Data is protected through layered technical and organisational measures under the Information Security Policy: encryption in transit and at rest; role-based access control, least privilege and MFA; firewalls, network controls and segregation of production and development environments; regular patching and monitoring; logging and regular log review; daily encrypted backups stored in secure, geographically separate locations and regularly tested; a defined incident response process with notification to the CGA and data protection authorities typically within 72 hours for material incidents; vendor due diligence and contractual security obligations; device and remote working controls; and staff security and data protection training at onboarding and on an ongoing basis.
Visual elements	57. What websites, domains, mobile applications, or software interfaces are used?	The Operator operates two brands under licence OGL/2024/358/0707: Space Casino at www.spacecasino.com and Xtreme at www.xtreme.game. The websites are accessible via desktop and mobile browsers, with the responsible gaming and account functionality available through the website and/or application interfaces.

	58. What branding, logos, license information, game pages, account screens, responsible gaming messages, warnings, pop-ups, banners, bonus displays, payment screens, terms links, complaints information, and footer information are shown?	Players are shown: brand identity (Space Casino / Xtreme branding and logos); the Operator's licence details and the CGA digital seal in the website footer; a clear visual indication that gambling by minors is prohibited (18+); a clear and visible link to the Responsible Gaming Section on the homepage and in the footer, together with links to gambling addiction support resources; links to the Terms and Conditions (no more than one click from the homepage) and the Privacy Policy; complaints contact information (complaints@spacecasino.com / complaints@xtreme.game) and escalation information; the game lobby and game pages with per-game rules available in the game interface; account screens including balance, transaction and gameplay history and responsible gaming tools; cashier/payment screens displaying applicable limits and any disclosed fees; and bonus displays with promotion-specific terms. All marketing content includes a responsible gaming message and 18+ warning.
	59. Are visual elements consistent across desktop and mobile versions?	Yes. The same content, notices, responsible gaming tools and terms apply across desktop and mobile interfaces of each website; presentation is adapted responsively to the device. Required notices (18+, licence details, CGA seal, responsible gaming links) are displayed in the footer of both desktop and mobile versions.
	60. Are legally required notices clearly visible?	Yes. The footer of each website displays the prohibition of underage gambling (18+), the Operator's licence details, the CGA digital seal, a link to the Responsible Gaming Section and links to gambling addiction support services. The Responsible Gaming Section is accessible from the homepage footer and side menu, and the Terms and Conditions are accessible no more than one click from the homepage. Responsible gaming information is provided in English and the language of the target market, with the English version prevailing.
	61. Are game rules, risks, odds, limits, and responsible gaming tools easy to find?	Yes. Game rules are available within each game interface before play; responsible gaming information, risk information and the self-assessment tool are available in the Responsible Gaming Section, reachable from the footer and side menu; responsible gaming limits and tools are accessible through account settings and on request via support; and applicable payment limits are displayed in the cashier. Game-specific odds and RTP display details are maintained in the Games Register.

	62. How are changes to visual elements reviewed and approved?	Material changes to player-facing content are reviewed for compliance before release: marketing and promotional content must comply with the Responsible Gambling Policy (including the required responsible gaming message and 18+ warning, and the prohibitions on misleading or pressuring content), and bonus terms must be fair, unambiguous and available within one click. Website changes follow the change control and segregation-of-environments requirements of the Information Security Policy, and the Key Compliance Officer's monthly compliance reviews provide ongoing oversight. Third parties involved in marketing are subject to due diligence and are required to comply with the Operator's policies.
Technical measures to prevent banned persons from playing	63. Which categories of banned or prohibited persons are blocked?	The following categories are blocked or refused: minors (under 18, or the higher legal age of the player's jurisdiction); self-excluded players (including their detected duplicate accounts); players excluded by the Operator; persons with a positive sanctions match; confirmed PEPs, PEPs by association and Special Interest Persons (the Operator has no risk appetite for these as customers); persons providing false or third-party identities or payment methods; duplicate accounts; players in restricted or sanctioned jurisdictions; accounts restricted for AML reasons (e.g. outstanding CDD/ECDD); and persons reasonably assumed to be vulnerable, in accordance with the Responsible Gambling Policy.
	64. How does the operator identify banned persons during registration, login, deposit, or gameplay?	At registration: the registration form requires a date of birth and it is impossible to enter a date of birth that would make the customer under 18; the player must confirm they are 18 or over; and duplicate account controls check for matches on first name, last name, date of birth, IP address and payment method. At first deposit: all customers are screened against the LexisNexis PEP, sanctions and adverse media databases, with a positive PEP or sanctions match automatically blocking the account. Ongoing: all customers are added to LexisNexis ongoing monitoring and rescreened every 24 hours; identity documents are verified at defined thresholds (NAf 4,000) and in all cases before the first withdrawal; automated systems detect duplicate or linked accounts through shared IP addresses, device identification, matching personal details and payment method overlap; and login is blocked for self-excluded and cooling-off accounts.

	65. Are exclusion lists, self-exclusion databases, age verification systems, sanctions checks, duplicate account checks, geolocation tools, identity verification tools, or device/IP checks used?	The Operator uses: internal exclusion records applied across all of its domains; LexisNexis Compliance Lens for PEP, sanctions and adverse media screening with 24-hour ongoing monitoring; age verification through date-of-birth controls and government-issued identity documents (with secondary measures such as electronic verification, payment validation, database checks and selfie/liveness verification available); duplicate account detection (name, date of birth, IP, payment method, device identifiers); identity verification tools per the AML Policy; and device/IP monitoring. Access from restricted jurisdictions may be blocked. The Operator does not currently participate in a national or central cross-operator self-exclusion database; self-exclusion confirmation emails remind players to self-exclude from other sites.
	66. How often are checks performed?	Age and duplicate checks are applied in real time at registration; PEP/sanctions/adverse media screening is performed at first deposit; ongoing PEP and sanctions rescreening runs every 24 hours for all customers; identity verification is triggered at NAf 4,000 cumulative transactions, in high-risk scenarios, and before the first withdrawal in all cases; transaction and behavioural monitoring operates continuously through automated alerts and manual review; and exclusion status is enforced at every login and deposit attempt.
	67. What happens if a banned person attempts to register or play?	Registration is refused where the date of birth indicates a minor. If an account is later found to belong to a minor, it is closed immediately, winnings are forfeited and net deposits refunded subject to legal requirements, and the system prevents further accounts with similar details. A positive PEP or sanctions match automatically blocks the account pending MLRO instruction, and the business relationship is terminated for confirmed PEPs, SIPs and sanctioned persons. Accounts created during self-exclusion are closed immediately, with any balance returned after verification where permitted. Attempts may also give rise to an Unusual Transaction Report and, where appropriate, disclosure to the FIU Curaçao.

	68. Are accounts suspended automatically or manually?	Both. Automatic controls include the registration age block, automatic blocking on positive PEP/sanctions matches, enforcement of self-exclusion and cooling-off (login and deposit blocks), and automated restriction where responsible gaming limits are reached. Manual suspensions and restrictions are applied by Compliance, the MLRO or senior management following review – for example pending verification, during investigations, on ECDD failure (account closed if ECDD is not completed within 1 month), or where documentation requested at the NAF 4,000 threshold is not received within 30 days (account fully restricted).
	69. How are attempted breaches recorded and reported internally?	Attempted breaches are logged in the back-office system against the customer record (including duplicate account detections, blocked registrations, screening matches and exclusion breaches) and, where they constitute security incidents, in the Incident Log. Staff escalate concerns to the MLRO using the internal Unusual Transaction Report process (acknowledged within 24 hours, reviewed within 48 hours), and the MLRO determines whether disclosure to the FIU Curaçao is required. Underage gambling attempts are documented with the account closure details. Records are retained and available for internal review and CGA inspection, and material incidents are reported to the CGA, typically within 72 hours.

Technical infrastructure diagram	70. Does the manual include a clear diagram of the platform architecture?	Yes – the technical architecture is set out in the summary diagram below. Player device (desktop / mobile browser) → Brand websites: www.spacecasino.com (Space Casino) / www.xtreme.game (Xtreme) → Web and network security layer: firewalls and network controls; TLS 1.2+ encryption; session timeout controls → Hub88 – third-party PAM (player account management) and aggregation platform: game lobby, player accounts, back-office administration → Hosting: Amazon Web Services, region eu-central-1 (Frankfurt, Germany); underlying facilities are AWS's Frankfurt availability-zone data centres → Player account and wallet ledger: balances, responsible gaming limits, exclusion status → Records: player account records, gaming transaction records, financial transaction records → Integrations: – Game providers (game content, outcome determination, game logs) – PSPs – fiat deposits and withdrawals: Payment IQ, Brite, AstroPay, PayRetailers, Gigadat, InPay – KYC / AML / sanctions screening providers, including LexisNexis Compliance Lens – PEP, sanctions and adverse media screening (24-hour ongoing monitoring) – Customer support and back-office systems (email / live chat) → Logging, monitoring and audit trails: user access, administrative actions, financial transactions → Backup / restoration arrangements: at least daily, encrypted, stored in secure geographically separate locations, regularly tested; disaster recovery and business continuity arrangements → CGA record export/access process: records searchable and exportable for production to the CGA; CGA portal requests received by the Managing Director and coordinated with the Key Compliance Functionary. Note: The Operator does not currently accept crypto-assets; a planned operator-managed crypto payment and wallet-control environment is not currently live and is therefore not shown.
----------------------------------	--	---

	71. Does the diagram show hosting, servers, databases, payment systems, game providers, platform providers, firewalls, APIs, back-office systems, monitoring tools, data centers, backup systems, and third-party integrations?	The architecture summary above shows the hosting and platform layer, player account/wallet and records databases, payment systems (PSPs), game providers, the platform provider, firewalls and security controls, integration points (APIs) with third parties, back-office systems, logging and monitoring, backup arrangements and third-party integrations. Named providers and locations: Hub88 (third-party PAM and aggregation platform), hosted on Amazon Web Services, region eu-central-1 (Frankfurt, Germany); underlying facilities are AWS's Frankfurt availability-zone data centres.
	72. Does it identify which systems are critical to the operation?	Yes. The systems critical to the operation are: the gaming platform (including the player account and wallet ledger); the player, gaming and financial records databases; payment processing integrations (PSPs); compliance screening (LexisNexis); logging, monitoring and audit trail systems; and backup and recovery infrastructure. The Information Security Risk Register specifically identifies PSP failure, third-party platform failure or breach, and platform downtime or infrastructure outage among the principal operational risks.
	73. Does it show where player data, transaction data, and gaming data are stored?	Player, gaming transaction and financial transaction data are stored within the gaming platform's databases (player account management and back-office), with copies in encrypted backups held in secure, geographically separate locations. Storage locations: Hub88 platform databases hosted on Amazon Web Services, region eu-central-1 (Frankfurt, Germany), with encrypted backups in secure, geographically separate locations.
	74. Does it show data flows between systems?	Yes. The principal data flows are: player device to website over TLS-encrypted connections; website/platform to game providers (game sessions, bets and outcomes); platform to PSPs (fiat payment authorisation and settlement); platform to LexisNexis (screening queries and ongoing monitoring alerts); platform to the wallet ledger and records databases; records to logging/audit systems; and databases to encrypted backups. These flows are shown in the architecture summary at Q70.

	75. Does it identify system owners or responsible parties?	Governance responsibilities are defined in the Information Security Policy: the Board of Directors holds ultimate accountability; the Key Compliance Function (KCF) ensures CGA compliance and oversees incident reporting; the Information Security / IT function implements and maintains security controls and monitors systems; and the Risk Register assigns named owners (IT, KCF, Operations) to specific risks. Third-party providers are responsible for their respective systems under contract.
Restoration possibilities in technical emergencies	76. What types of emergency situations are covered?	The incident response and business continuity framework covers data breaches, unauthorised access, system compromise, and fraud or suspicious activity, together with the operational scenarios identified in the Risk Register: platform downtime or infrastructure outage, failure or breach of the third-party platform, PSP failure or delays, internal error leading to data exposure, unauthorised privileged access, and compromise of player accounts. Incidents are classified Low, Medium or High/Critical according to whether player data, funds or systems are affected.
	77. Are server failure, cyberattack, data loss, payment outage, game provider outage, platform outage, network failure, database corruption, and disaster recovery scenarios addressed?	Yes. Server and infrastructure failure, cyberattack (system compromise, unauthorised access, credential attacks), data loss (addressed through daily encrypted, geographically separate, regularly tested backups), payment outages (PSP failure is a specifically identified risk, mitigated by transaction monitoring and PSP diversification), game provider and platform outages (mitigated through provider SLAs, hosting redundancy and contingency planning), network failure and database corruption (addressed through backup and recovery arrangements) are all covered by the incident response, disaster recovery and business continuity arrangements maintained under the Information Security Policy.
	78. What backup procedures are in place?	Data is backed up at least daily. Backups are encrypted, stored in secure, geographically separate locations, and regularly tested. The Operator maintains disaster recovery procedures and business continuity arrangements, and defines disaster recovery expectations with its hosting and platform providers, whose uptime is monitored.
	79. How often are backups made?	Backups are made at least daily, in accordance with the Information Security Policy.

80. Where are backups stored?	Backups are stored encrypted in secure, geographically separate locations. Backup storage locations/providers: provided through the Hub88/AWS environment and associated operational continuity processes.
81. What recovery time objectives and recovery point objectives apply?	Formal recovery time objectives (RTO) and recovery point objectives (RPO) are not stated in the Information Security Policy. The at-least-daily backup cycle provides a maximum data-loss window of 24 hours. The applicable RTO and RPO values are maintained in the disaster recovery procedures.
82. Who is responsible for activating recovery procedures?	The Information Security / IT function is responsible for executing recovery under the incident response process (identify, contain, investigate, remediate, recover, document), with the Key Compliance Function overseeing incident reporting and regulatory communication, and escalation to senior management for High/Critical incidents. The Board holds ultimate accountability. Where an incident is material, the CGA is notified, typically within 72 hours.
83. How are players informed during service interruptions?	Affected users are notified where appropriate, in accordance with the incident response communication requirements, and internal stakeholders are informed promptly. Communication channels include on-site notices on the websites and direct communication by email or support channels (email and live chat). The Terms and Conditions inform players that the websites may be temporarily unavailable due to maintenance, technical issues or circumstances outside the Operator's control.
84. How are unfinished games, pending bets, deposits, withdrawals, and balances handled after restoration?	Following restoration: interrupted games are resolved on the basis of the official system records maintained by the Operator and the relevant game provider, and incomplete wagers are refunded where appropriate in accordance with the applicable game rules; bets affected by a malfunction may be voided together with winnings derived from it. Player balances are verified against the wallet ledger, game logs and transaction records, and corrected where errors are identified. Pending deposits and withdrawals are reconciled against PSP settlement reports, and any manual adjustments are documented with an audit trail. Players are informed of the treatment of affected transactions, and disputes arising are handled under the complaints process.

Responsible gaming implementation	85. What responsible gaming policy applies?	The Operator applies its Responsible Gambling Policy which applies across all brands and domains operated under the licence, including Space Casino (www.spacecasino.com) and Xtreme (www.xtreme.game). The policy implements the responsible gaming requirements of the LOK and CGA guidance and covers: protection of minors and vulnerable persons; player information and the Responsible Gaming Section; responsible gaming tools (deposit, wager and loss limits, reality checks, Take a Break / cooling-off, self-exclusion and self-assessment); behavioural monitoring and intervention; staff training; marketing restrictions; and record keeping. It operates alongside the AML and Fraud Policy, Privacy Policy and the Terms and Conditions of each brand, and its operation is reviewed monthly by the Key Compliance Officer.
	86. How are players informed about responsible gaming risks?	The Operator informs players about responsible gaming risks through a clearly identifiable and easily accessible Responsible Gaming Section on the website and/or application. The Responsible Gaming Section provides clear and understandable information enabling players to make informed decisions about their gambling behaviour. It includes information on gambling-related risks, signs of problematic gambling, the prohibition of underage gambling, available responsible gaming tools, and how players may contact the Operator regarding responsible gaming concerns by email or chat. A clear and visible link to the Responsible Gaming Section is displayed on the homepage and in the footer of the website or application. The Responsible Gaming Section is also referenced in the Terms and Conditions, which are accessible no more than one click away from the homepage. The information is made available in English and in the language of the Operator's target market, with the English version prevailing in case of discrepancy. The footer of the website or application includes a clear visual indication that gambling by minors is prohibited, the Operator's licence details, the CGA digital seal, a link to the Responsible Gaming Section, and links to gambling addiction support resources, including international and, where available, local support services.

	87. What tools are available to players, such as deposit limits, loss limits, wager limits, session limits, time-outs, reality checks, self-exclusion, account closure, and cooling-off periods?	The Operator makes responsible gaming tools available to players through the Responsible Gaming Section of the website or application. These tools include, at a minimum, deposit limits, cooling-off periods, self-exclusion, access to betting and wagering history, and player self-assessment resources. Players may set deposit limits for daily, weekly, or monthly periods. Once a deposit limit is reached, the player cannot make further deposits until the relevant period resets. Any request to make a deposit limit more restrictive takes effect immediately, while any request to make a limit less restrictive or to remove it is subject to a 7-day cooling-off period, after which the player must confirm the change before it takes effect. Players may activate a cooling-off period of 24 hours, 7 days, 1 month, or 3 months. During a cooling-off period, the player is restricted from gambling activity in accordance with the selections made, while funds remain available for withdrawal. Players may also self-exclude for a period of 1 year, 3 years, 5 years, 10 years, or lifetime. Self-exclusion applies to all gambling activity and all brands or domains operated under the Operator's licence. During self-exclusion, the player's account is closed, login is blocked, deposits and wagering are prohibited, and direct marketing is stopped. The Operator may also offer additional tools based on its risk profile, including loss limits, wager limits, time limits, session limits, player-activated reality checks, pop-up reminders, real-time session timers, and access to internet filtering tools.
--	---	---

	88. How does the operator detect risky or problematic gambling behavior?	The Operator operates behaviour tracking controls to identify signs of risky or problematic gambling behaviour. Monitoring is performed through a combination of system-based alerts, player account data, transactional monitoring, and observations by frontline staff such as customer support, VIP, and responsible gaming personnel. The Operator assesses risk holistically and does not rely on a single indicator alone unless the circumstances justify immediate action. Monitoring factors include sudden or unexplained increases in deposit or wagering frequency, repeated failed transactions due to insufficient funds, repeated withdrawal reversals, inexplicably extended play sessions, increased or agitated communication with customer support, frequent changes to responsible gaming tools, use of cooling-off periods, players maxing out credit cards, and attempts to open multiple accounts to bypass limits or exclusions. Where appropriate, the Operator may use platform features, in-game tools, automated alerts, artificial intelligence, machine learning, or manual review to support the detection of at-risk behaviour.
	89. Are player interactions documented?	All responsible gaming interactions are documented in the Player Account Management system or another designated internal system. This includes interactions initiated by the player and by the Operator. Records include the date and time of the interaction, the staff member or system involved, the indicator or concern identified, the information provided to the player, tools discussed or applied, any player response, escalation steps, account restrictions, temporary suspensions, exclusions, and follow-up actions. Operator-initiated exclusions are formally documented and retained for at least five years. Records are maintained so that they can be reviewed internally and made available to the CGA upon request where required.

	90. How are vulnerable players protected?	The Operator protects vulnerable players by implementing proactive responsible gaming controls designed to prevent and mitigate gambling-related harm. A vulnerable person includes a minor, a person who has insufficient control over gambling behaviour, a person banned from gambling by force or at their own request, and a person declared bankrupt. The Operator does not knowingly permit a person who can reasonably be assumed to be vulnerable to participate in games of chance. Where a player displays behaviour suggesting vulnerability or gambling-related harm, the Operator initiates appropriate responsible gaming intervention. This may include informing the player of available tools, directing the player to support resources, applying mandatory deposit limits, temporarily suspending the account, or excluding the player where the risk is severe or persistent. Marketing and advertising are not directed at vulnerable persons and must not portray gambling as a solution to financial, emotional, or mental difficulties. The Operator also ensures that bonuses or promotions are not used to encourage excessive gambling or to discourage the use of responsible gaming tools.
	91. How does the operator prevent minors and excluded persons from gambling?	The Operator prohibits any person under the age of 18 from registering, depositing, wagering, or otherwise participating in games of chance. During registration, the player must enter their date of birth and confirm that they are over 18 by selecting a designated checkbox. Additional checks are performed to obtain sufficient certainty that the player is not a minor. At a minimum, government-issued valid identification, such as a passport, national ID card, or driver's licence, is verified upon reaching specified thresholds and in all cases before the first withdrawal. The Operator may also use secondary verification measures such as electronic verification systems, payment validation, government or third-party database checks, and selfie or liveness verification. If the Operator becomes aware that a player is a minor, the account is closed immediately, the reason for closure is communicated, and the civil law implications are considered, including potential refund of deposits and forfeiture of winnings. Records of age verification checks and outcomes are retained and made available for regulatory review.

	92. How are responsible gaming obligations under Articles 2.2(3), 5.4, and 5.6 of the LOK implemented operationally?	The Operator implements responsible gaming obligations operationally through a documented Responsible Gaming Policy, player-facing Responsible Gaming Section, responsible gaming tools, internal monitoring procedures, escalation protocols, and staff training. The Operator integrates responsible gaming principles into its business model and takes proactive steps to protect vulnerable persons, promote responsible gambling, and prevent or mitigate problem gambling behaviour. The Operator appoints a person responsible for responsible gaming tasks within the organisation. Until a dedicated responsible gaming person is appointed, the Compliance Officer responsible for non-AML compliance performs this function. The responsible gaming function reports to management at least once every 12 months on the effectiveness of the policy and operational procedures and recommends any required enhancements. Material changes to the Responsible Gaming Policy are reported to the CGA. Operationally, the Operator ensures that players can access responsible gaming information, set deposit limits, activate cooling-off periods, self-exclude for at least one year, access self-assessment tools, and obtain support resources. The Operator also implements behaviour tracking and intervention procedures, prevents minors and excluded persons from gambling, trains relevant staff, and ensures that advertising and marketing comply with responsible gaming standards. The Operator provides responsible gaming training to relevant staff, including customer support, VIP, marketing, compliance, and responsible gaming personnel. Training covers recognition of gambling distress, signs of problematic gambling, handling sensitive player conversations, escalation of responsible gaming concerns, use of responsible gaming tools, directing players to support resources, preventing marketing to vulnerable players, and documenting responsible gaming interactions. Staff who interact with players are trained to respond professionally, neutrally, and without encouraging continued play where responsible gaming concerns exist. The Operator ensures that marketing and advertising comply with responsible gaming standards. Marketing does not knowingly or deliberately target
--	---	---

		vulnerable persons, minors, self-excluded players, or persons showing indicators of problematic gambling. Advertising does not portray gambling as an investment, a route to financial success, a solution to financial or emotional difficulties, or a substitute for well-being. Marketing does not misrepresent the role of chance, does not suggest that skill can influence purely chance-based games, and does not include minors, explicit content, or links between gambling and harmful behaviours. Bonuses and promotions are communicated transparently with clear terms and conditions and are not used to encourage excessive gambling. All advertising includes a clearly visible responsible gaming message or slogan. Affiliates, influencers, ambassadors, representatives, and other third parties involved in marketing are informed of the Operator's Responsible Gaming Policy and are required to comply with it.
General Terms and Conditions	93. What is the current version number and date of the Terms and Conditions?	Space Casino (www.spacecasino.com): Terms and Conditions version 1.0, effective June 2026. Xtreme (www.xtreme.game): Terms and Conditions version 1.0, effective June 2026. Both are issued by Luminect Limited B.V. under licence number OGL/2024/358/0707.
	94. Are the Terms and Conditions included in full or attached as an annex?	The most recent text of the general Terms and Conditions for each brand (Space Casino and Xtreme, both version 1.0, June 2026) is maintained as controlled documents and may be included as annexes to the Operational Manual or provided separately with the submission pack, in accordance with Article 5.9, paragraph 1(h) of the LOK.
	95. Do they match the version published on the website or application?	Yes. The Terms and Conditions in this manual (Space Casino Terms and Conditions v1.0, June 2026, and Xtreme Terms and Conditions v1.0, June 2026) match the versions published on the Space Casino and Xtreme websites. Under the Terms and Conditions, updated versions are published on the website and take effect from the stated effective date, and previous versions are available to players on reasonable request.

	96. How are updates to the Terms and Conditions approved?	Amendments are made where necessary for legal, regulatory, operational, security or commercial reasons, in accordance with clause 18 of the Terms and Conditions. Updates are reviewed by the compliance function for consistency with the Operator's policies and regulatory obligations and approved at senior management level before publication, consistent with the Operator's governance framework under which the board approves policies. Changes do not apply retrospectively unless required by law, necessary to correct errors, or not disadvantageous to players. Approval records for Terms and Conditions updates are maintained in the Operator's document control records.
	97. How are players notified of material changes?	Updated Terms and Conditions are published on the website and become effective from the date specified in the updated version. Where material changes are made, the Operator takes reasonable steps to notify players through the website, email or other appropriate communication channels before the change becomes effective. The Privacy Policy likewise commits to notifying players of material changes via the website, email or other suitable means before they take effect.
	98. How is player acceptance recorded?	During registration, players must actively confirm acceptance of the Terms and Conditions by selecting the confirmation checkbox before an account can be created; this acceptance is recorded against the player's account. Continued use of the website following the effective date of updated Terms constitutes acceptance of the updated version. Registration records, including the acceptance confirmation and timestamp, are retained within the player account records.

	99. Do the Terms and Conditions cover eligibility, account registration, deposits, withdrawals, bonuses, gameplay rules, responsible gaming, complaints, suspension, termination, data use, and governing law?	Yes. Both the Space Casino and Xtreme Terms and Conditions (which are materially identical apart from brand, domain and contact details) cover: eligibility and minimum age (clause 4.1–4.3); account registration, one-account rule and player information (4.4) and KYC verification (4.5, 5); deposits and withdrawals, chargebacks and third-party payment restrictions (6) and customer funds (7); bonuses and promotions, including wagering requirements and bonus abuse (8); responsible gambling and the available tools (9); gameplay and fair gaming, game rules, malfunctions and game results (10); account security, suspension and closure (11); complaints and dispute resolution, including ADR escalation (12); data protection, AML monitoring, record retention and third-party disclosure (13); prohibited activities (14); and governing law – the laws of Curaçao (17).
Dispute settlement with players	100. What qualifies as a complaint or dispute?	A complaint is any written expression of dissatisfaction submitted by a registered player regarding the Operator's services, decisions, terms, conduct, or any incident connected to the player's participation in games of chance, where the player expects a response or resolution. This includes, but is not limited to, complaints relating to deposits, withdrawals, bonus terms, account closures or restrictions, alleged game errors or unfair game outcomes, responsible gaming matters, treatment of player balances, KYC and verification, data protection, technical or software issues, AML concerns, minors, fraudulent games or practices, licensing or regulatory issues, and unfair terms and conditions. A dispute is a complaint that has not been resolved to the player's satisfaction through the Operator's internal complaints process and has been escalated internally, to an independent ADR provider, or to a court of law.

	101. How can players submit complaints?	Players may submit complaints free of charge within six months from the settlement of the bet or the incident giving rise to the complaint. For peer-to-peer games, such as poker, and ante-post fixed odds betting, the six-month period starts from the settlement of the bet or conclusion of the relevant event, rather than the placement of the wager. Complaints may only be submitted by the registered player. Complaints may be submitted through the designated complaints channel for each brand (complaints@spacecasino.com for Space Casino; complaints@xtreme.game for Xtreme), as published in the Terms and Conditions, in addition to customer support via email and live chat. The submission process operates in accordance with the Operator's Complaints Policy and applicable CGA requirements.
	102. Which communication channels are available?	The Operator offers customer support through email and/or live chat. Players may submit complaints through the designated complaints channel and, where made available, through an official Complaint Submission Form. Information on how to contact the Operator, how to access the Complaint Submission Form, and how to escalate unresolved complaints is included in the Terms and Conditions and made visible and accessible on the website, either as a standalone complaints link or document.
	103. What information must players provide?	Where a Complaint Submission Form is used, it requires, at a minimum, the player's name, address, place of residence, account number where applicable, the date of the complaint, the date of the disputed event, and a description of the conduct, decision, transaction, or event being disputed. The form may also include pre-determined complaint categories to assist classification and handling. The Operator may request supporting documents or additional information that are reasonably required to investigate and resolve the complaint. Any request for additional information must be proportionate and relevant to the complaint.

	104. What internal department handles complaints?	Complaints are handled by the Operator's Customer Support in the first instance. Complaints involving specific subject matter are escalated to the relevant internal department, such as Payments, Gaming Operations, KYC/Verification, AML/Compliance, Responsible Gaming, Technical Support, Legal, or Management. Responsible gaming complaints are prioritised and handled with appropriate involvement of trained Responsible Gaming or Compliance personnel.
	105. What are the timelines for acknowledgement, investigation, response, and escalation?	Responsible gaming complaints are treated as priority matters. Within two (2) days of receiving a responsible gaming complaint, the Operator confirms receipt in writing, explains how the complaint will be processed, and provides the expected timeline for resolution. The Operator uses best efforts to resolve responsible gaming complaints within five (5) business days. If more time is required to make a reasonable and informed decision, the player is informed of the delay, which may not exceed two (2) weeks. If the delay is caused by lack of information or slow response from the player, the resolution period may be extended by no more than a further two (2) weeks. For all other complaints, the Operator confirms receipt in writing within one (1) week, explains how the complaint will be processed, and provides the average timeline for resolution. The Operator assesses and responds to such complaints within four (4) weeks. If necessary, due to complexity or lack of information, this period may be extended once by an additional four (4) weeks, provided the player is informed in writing before the original period expires. If the player is dissatisfied with the final outcome, the player is informed of the right to escalate the complaint to an independent ADR provider free of charge.

	106. How are complaint decisions documented?	The Operator documents all complaints and complaint decisions in a complaint register. Each record includes the player details, account number (where applicable), complaint date, disputed event date, complaint category, summary of the issue, supporting documents requested and received, internal departments involved, investigation steps, decision, outcome, response date, escalation history, and whether the complaint was upheld, rejected, settled, pending, unresolved, referred to ADR, or subject to legal action. The player always receives a final determination in writing. The written response includes either a reasoned final assessment of the complaint and outcome, with supporting evidence where necessary or applicable, or detailed reasons why the complaint is not being handled. Records of unresolved complaints and complaints escalated to ADR or legal proceedings are retained for the required period, and the CGA may request access to complaint and dispute records at any time.
--	--	---

	107. How are disputes regarding bets, winnings, payments, account closures, bonuses, responsible gaming, or verification handled?	Complaints and disputes are investigated according to their subject matter and escalated to the relevant internal department. Bet and game outcome disputes are reviewed against game logs, transaction records, game rules, provider records, settlement data, and any relevant technical evidence. Winnings and balance disputes are reviewed against the player wallet, game history, payout rules, bonus rules, and payment records. Deposit and withdrawal complaints are reviewed by Payments and Compliance against transaction references, payment provider records, AML/KYC status, withdrawal rules, and any relevant delays or restrictions. Account closure or restriction complaints are reviewed against the Terms and Conditions, account history, security records, responsible gaming records, AML/KYC findings, and compliance grounds for the action taken. Bonus complaints are reviewed against the applicable bonus terms, wagering requirements, eligibility criteria, communications, and player activity. Responsible gaming complaints are prioritised and reviewed by trained staff, particularly where the complaint concerns vulnerable players, self-exclusion, cooling-off, or the timely implementation of responsible gaming measures. KYC and verification complaints are reviewed against the Operator's verification requirements, documents submitted, requests for additional information, and any applicable legal or regulatory obligations. In all cases, the Operator provides a written, reasoned decision and does not use the complaints process to unfairly delay legitimate withdrawals or avoid valid obligations to the player. In summary, the process for all such disputes is: (1) receipt and logging of the complaint in the complaint register; (2) written acknowledgement with an explanation of the process and expected timeline; (3) investigation by the relevant department against the records identified above, with any requests for further information kept proportionate; (4) a written, reasoned final decision to the player within the applicable timeframe; and (5) where the player remains dissatisfied, escalation to the Operator's independent ADR provider free of charge, with records of the escalation retained and available to the CGA.
--	--	--

	108. Are unresolved complaints escalated to a CGA-approved contracted ADR provider?	Unresolved complaints are escalated, free of charge to the player, to the Operator's contracted CGA-approved ADR provider once the internal complaints procedure has been exhausted and the Operator has issued its final response. The ADR provider named in the Terms and Conditions of both brands (clause 12.3) is EGIS – FZCO, Unit 22105-001, IFZA Business Park, DDP, Dubai, United Arab Emirates (https://egis-adr.com), which operates independently of the Operator. ADR referrals are authorised by senior management and recorded in the complaint register.
Digital records of player information	109. What specific player records are maintained?	The Operator maintains digital records of: identity and registration data (name, date of birth, address, contact details, account ID); KYC/verification records (POI/POA documents, verification outcomes, payment method ownership evidence, source of funds / source of wealth documentation where obtained); screening records (PEP, sanctions and adverse media results and ongoing monitoring alerts); customer risk assessments, risk profile reviews and Unusual Transaction Reports; account status, exclusion and cooling-off status and responsible gaming limits; communications records including support correspondence, chat logs and full transcripts of ECDD-related conversations; complaints and their outcomes in the complaint register; responsible gaming interactions, trigger reviews and interventions; and account change history with audit trails.
	110. Are identity details, registration data, verification records, account status, exclusion status, limits, communications, risk indicators, complaints, responsible gaming interactions, and account changes retained?	Yes. All of the listed categories are retained: identity details and registration data; verification records and outcomes; account status (active, restricted, suspended, closed); exclusion and cooling-off status, applied across all Operator domains; responsible gaming limits and their change history; communications (email, chat, complaint correspondence, recorded ECDD conversations); risk indicators (customer risk ratings, screening alerts, monitoring flags); complaints and outcomes; responsible gaming interactions (logged in the back-office system, including tool changes, trigger reviews and self-exclusion events); and account changes, which are captured in the system logs of user and administrative actions.

	111. Are records complete, accurate, searchable, and exportable?	Records are maintained digitally in the platform back-office and compliance systems in a complete and accurate form, protected against unauthorised alteration by access controls and audit logging. They are searchable by player and account identifiers and exportable in readable formats for internal review, audit and production to the CGA on request. Duplicate search and account review functionality is used routinely in compliance reviews (as reflected in the Risk Profile Review procedure).
	112. How long are records retained?	CDD/ECDD and associated AML records are retained for a minimum of 5 years after the business relationship ends. Crypto-asset record retention requirements under the Crypto Asset Policy will apply only if crypto payments are implemented in future. Complaint records are retained for a minimum of 3 years. Operator-initiated exclusion records are retained for at least 5 years. Other personal data is retained as long as necessary for the purposes collected, in line with the Privacy Policy, and then securely deleted, anonymised or aggregated.
	113. Who can access or amend the records?	Access is restricted on least-privilege, role-based principles to authorised personnel (customer support, payments, compliance/MLRO, responsible gaming and IT administrators as appropriate), with MFA required for back-office access. Amendments are made only by authorised staff through controlled back-office functions and are captured in logs of user access and administrative actions; privileged access is monitored and logged. Confidential AML records, including UTRs, are held by the MLRO with restricted access to protect against tipping off.
	114. Are audit trails maintained?	Yes. Logs are maintained for user access, administrative actions and financial transactions; they are stored securely and reviewed regularly. Responsible gaming actions, account restrictions and compliance decisions are recorded against the customer account in the back-office system, providing an auditable history available to the CGA on request.

Digital records of gaming transactions	115. Are all bets, stakes, wagers, game rounds, odds, outcomes, wins, losses, cancellations, refunds, jackpots, bonuses used in gameplay, and game session details recorded?	Yes. The platform and game providers record all gameplay activity, including bets, stakes and wagers, game rounds, outcomes, wins and losses, cancellations and refunds (including wagers refunded following interrupted games), bonus funds used in gameplay and wagering progress, and game session details (game, time of play, session length and device data). These records constitute the official game records referred to in the Terms and Conditions. The detailed field schema and jackpot-specific records are maintained in the platform specification and the Games Register.
	116. Do records identify the player, date, time, game, transaction ID, amount, currency, result, and balance impact?	Yes. Gaming transaction records identify the player account, date and time, the game played, transaction identifiers, amounts staked and won, the currency, the game result and the impact on the player's balance, enabling each entry in the wallet ledger to be traced to the underlying game round. The field-level specification is maintained in the platform documentation.
	117. Can records be reconstructed in case of dispute or regulatory inspection?	Yes. Official game records, transaction logs and system records maintained by the Operator and/or the relevant game provider prevail in the event of any discrepancy, dispute or technical inconsistency, and are used to reconstruct events during complaint investigations (game outcome disputes are reviewed against game logs, transaction records, game rules, provider records and settlement data). Records are retained in accordance with regulatory requirements, protected by access controls and audit trails, and backed up daily, supporting reconstruction for regulatory inspection.
	118. Are game provider records reconciled with platform records?	Yes. Platform records are reconciled with game provider records, and provider records are used alongside platform records in dispute investigations; where discrepancies arise, the official system records prevail and balances are corrected with a documented audit trail.
Digital records of financial	119. Are deposits, withdrawals, reversals, chargebacks, payment failures, fees, currency conversions, crypto transactions, bonus credits, manual adjustments, and refunds recorded?	Yes. Financial transaction records currently cover fiat deposits, withdrawals, reversals, chargebacks, failed payments, fees, currency conversions, bonus credits and bonus-related adjustments, manual adjustments and corrections, and refunds. Crypto-asset transaction records will be added only if crypto payments are implemented in future. Transaction records are among the record categories the Operator commits to retain under the Terms and Conditions.

Availability of records to the CGA	120. Do records include date, time, amount, currency, payment method, payment provider, transaction reference, player account, status, and approval history?	Yes. Financial transaction records include the date and time, amount, currency, payment method, payment provider (PSP), transaction reference, the player account, transaction status, and the approval history where manual review or AML approval applied (for example, withdrawal approvals follow verification and compliance checks).
	121. Are financial records reconciled with payment service provider data and player wallet balances?	Yes. The Operator reconciles fiat settlement transfers, payment provider fees and customer account ledger entries, and reconciliations are documented and retained. The Operator maintains internal controls to ensure accurate recording and reconciliation of player balances, and PSP transaction data (Payment IQ, Brite, AstroPay, PayRetailers, Gigadat, InPay) is reconciled against the platform ledger, with the Payments team investigating delays and unusual flows.
	122. How are unusual transactions flagged?	Unusual transactions are flagged through a hybrid of automated and manual monitoring: automated systems flag key risk indicators such as deposit anomalies, mismatched payment details and high-volume transactions; defined thresholds trigger review (CDD at NAf 4,000 cumulative; MLRO risk profile review at NAf 5,000 or more in daily transactions; review where a withdrawal over NAf 1,000 follows a deposit that was not wagered); and staff report suspicions via the internal UTR process. All alerts are reviewed and escalated to the MLRO where appropriate (acknowledged within 24 hours, reviewed within 48 hours), who determines whether disclosure to the FIU Curaçao is required. Tipping-off safeguards apply throughout.
	123. Are the required records continuously accessible?	Yes. Player, gaming transaction and financial transaction records are maintained digitally within the platform and back-office systems and are continuously accessible to authorised personnel; responsible gaming and compliance records are accessible and auditable at the request of the CGA. Server/environment and data centre details are set out in the Server and Data Centre section (Q130–135).

124. Can the CGA obtain records without delay when requested?	Yes. CGA requests are received through the CGA portal. The Managing Director, being the Curaçao-based authorised portal user, has primary access to the portal, and the Key Compliance Functionary acts as the primary contact for the CGA. Records are produced promptly from the back-office and compliance systems, which support search and export by player and transaction identifiers. Incident-related information is provided to the CGA within the applicable notification timeframes (typically 72 hours for material incidents).
125. Are records stored in a format that is readable, complete, and exportable?	Yes. Records are stored digitally in complete form, protected against unauthorised alteration by access controls and audit trails, and can be exported from the back-office and compliance systems in commonly readable formats for production to the CGA.
126. Who is responsible for responding to CGA requests?	The Managing Director, being the Curaçao-based authorised portal user, has primary access to the CGA portal through which the CGA may log requests for information and documents. The Managing Director coordinates responses with compliance, technical and operational personnel as required. The Key Compliance Functionary (KCF), who also serves as MLRO, is the designated primary contact for the CGA and the FIU, ensures adherence to regulatory requirements, and coordinates the collation and delivery of requested records with the relevant departments. The board of directors holds ultimate accountability for regulatory compliance.
127. Are access logs and audit trails available?	Yes. Logs of user access, administrative actions and financial transactions are maintained, stored securely and reviewed regularly, and can be made available to the CGA on request, together with the Incident Log and compliance review records.
128. Are backup records also available?	Yes. Data is backed up at least daily; backups are encrypted, stored in secure, geographically separate locations, and regularly tested to confirm they can be restored. Backup copies of the required records can therefore be produced if primary records are unavailable.

	129. What procedures apply if the primary system is unavailable?	If the primary system is unavailable, the incident response process is activated (identify, contain, investigate, remediate, recover, document) and services and records are restored from the daily encrypted backups under the disaster recovery and business continuity arrangements. The CGA is notified of material incidents, typically within 72 hours, and the Key Compliance Function manages regulatory communication during the outage. Records requests received during an outage are fulfilled from backup records.
Server and data center requirement	130. Which server stores the required critical records? Is the server located in a Tier-IV certified data center? Is the data center registered in Curaçao?	The current critical records platform is Hub88, a third-party PAM and aggregation platform, hosted on Amazon Web Services in region eu-central-1, Frankfurt, Germany. The underlying facilities are AWS's Frankfurt availability-zone data centres. The relevant Tier-IV certification and Curaçao registration evidence is identified in Q131.
	131. What evidence confirms the certification and registration?	The relevant evidence comprises: • the Hub88 service/platform documentation; • AWS hosting-region confirmation for eu-central-1; • the data centre's Tier-IV certification; • evidence of the data centre's registration in Curaçao; • the hosting or service agreement identifying the server/environment and the records maintained on it.
	132. Which records are stored there?	The records maintained in the current critical records platform comprise player information, gaming transaction records and financial transaction records processed through Hub88, including the categories described in Q109–122.
	133. Are mirrored, backup, or replicated records also maintained?	Yes. The Operator's data is backed up at least daily; backups are encrypted, stored in secure, geographically separate locations and regularly tested. Backup, mirroring or replication arrangements are provided through the Hub88/AWS environment and associated operational continuity arrangements. Relevant data is backed up for business continuity, restoration and CGA availability purposes.
	134. Who manages the server?	The current critical records platform is operated by Hub88 as third-party PAM and aggregation provider, using AWS eu-central-1 hosting, under the Operator's third-party and vendor due diligence framework and contractual security obligations. Internal management responsibility sits with the Operator's Information Security / IT function, with oversight by the Key Compliance Function.

	135. What security, access control, monitoring, and business continuity measures apply?	The controls applying to the current critical records platform (the Hub88/AWS environment) follow the Information Security Policy: role-based access control with least privilege and multi-factor authentication; encryption of data in transit (TLS 1.2+) and at rest (e.g. AES-256); logging and monitoring of access and administrative actions with regular review; at least daily encrypted backups stored in geographically separate locations and regularly tested; the incident response process with CGA notification typically within 72 hours for material incidents; disaster recovery and business continuity arrangements; vendor due diligence, approved/time-limited/monitored vendor access and periodic vendor risk review; audit trails supporting CGA inspection; and the ability to export the records in a complete, readable format for CGA access.
--	---	---