

Curaçao Gaming Authority (CGA) OPERATIONAL MANUAL

Luckland – CasinoMidas.com

Version: 2.0

COMPANY INFORMATION

Legal Name: Luckland Group BV

Trading Name:

Website: www.casinomidas.com – www.jackmillion.com – www.spinsamba.com –
www.spingrande.com

Licence Number: OGL/2024/494/0671

Registered Address: Kaya Richard J. Beaujon z/n, Curacao

Under Curaçao's new gaming framework (the LOK), licence holders must maintain a detailed operational manual that provides clear guidance across every aspect of their activities.

Game Descriptions and Payouts

Verifiable under the websites of our 4 brands in Curacao:

www.casinomidas.com

www.jackmillion.com

www.spinsamba.com

www.spingrande.com

The sites broadly include a detailed description of all games offered, together with their stakes, payout structures, and the elements determining game outcomes. This ensures full transparency and consistency in how players engage with the games and understand their odds and rewards, additionally to our attached T&Cs.

Quality Control

Luckland should clearly document the quality control procedures used to monitor and verify the integrity of both games and supporting systems. This includes the technical testing and certification processes conducted by accredited laboratories, as well as any risk management measures designed to maintain reliability and fairness.

Technical Requirements

The manual should provide a full overview of the operator's technical infrastructure, including data storage methods, system architecture, and cybersecurity controls in place to safeguard information. It should also outline the restoration procedures to be followed in the event of a technical failure or emergency.

All gaming and financial transaction information must also be hosted within a Tier-IV certified data centre registered in Curaçao, ensuring access for the CGA to oversee operations, when requested.

Visual Elements

A description of the visual elements presented to participants through websites or applications should be included, ensuring clarity in how games are displayed and experienced.

Responsible Gambling

Licence holders should describe the technical and operational safeguards implemented to promote responsible gambling. These include systems that prevent access by prohibited or vulnerable individuals, self-exclusion options, and visibility of support resources. The framework must align with the Curaçao responsible gaming provisions established under the Ordinance.

Terms and Conditions

Comprehensive terms and conditions should be documented and made accessible to all players. These should set out fair rules, rights, and obligations, clearly defining the legal framework governing the gaming relationship under Curaçao law.

Dispute Resolution

The manual should define clear procedures for handling player complaints and disputes, ensuring that issues are addressed promptly and transparently. It should also describe the alternative dispute resolution (ADR) mechanism approved by the CGA, which provides independent oversight and ensures fairness in the resolution process.

Staff Training and Education

Finally, the manual should outline the operator's programme for annual staff training and ongoing education. This training should cover responsible gaming, anti-money laundering (AML), and operational integrity, ensuring that all personnel involved in gaming activities maintain high professional and ethical standards. In terms of company structure we have a total of 36 employees: 1 Head of Unit, 3 Department Heads (Risk, IT, DPO included), 4 Team Leads, 28 Agents (CS & VIP). With respect to Compliance Governance the key roles are the: MLRO, Compliance Officer and Responsible Gaming Officer. All Personnel is annually trained or even earlier, upon need.

Maintaining a thorough operations manual is essential for compliance and accountability in Curaçao.

Date of updating 2025 - 2026

	Question	Answer
--	----------	--------

G a m e s o f C h a n c e o f f e r e d (G a m e s R e g i s t e r	1. Which games are offered to players (casino games, sports betting, live casino, lotteries, bingo, poker, fantasy sports, crash games, or another category)?	(Please, see on the websites under question 2, for the full list) Luckland operates as an online gaming operator providing remote casino services under Curaçao regulatory oversight. The company provides online casino entertainment services using RNG-based games as supplied by Realtime Gaming (RTG). Please note that sportsbook, poker, or lottery products are “not” offered, currently .
	2. for each game type, what are the basic rules of play?	Please see them in more detail, through the following links to each game type: www.casinomidas.com www.jackmillion.com www.spinsamba.com www.spingrande.com

r)	3. Are any games supplied by third-party providers?	Please find below the breakdown of Luckland’s suppliers/aggregators per games a. Casino Aggregator (for Spingrande only): Reevo b. Sportsbook Provider (for Midas, Jack Million and Spin Samba): DELASPORT c. Sportsbook Back Office: Orbit (DELASPORT) Please note that no white-label arrangement is used. For the sake of completeness our Provider (for all games) is Realtime Gaming (RTG), namely Realtime Gaming, often abbreviated as RTG, which is a gambling software production society founded in 1998 in the US, specifically in Atlanta, Georgia. Bought in January 2007 by Hastings International - HBM Group, Realtime Gaming has moved its operative headquarters to Heredia, Costa Rica. To Luckland, Real Time Gaming offers downloaded games or online flash versions always in the world Top 5, together with important competitors such as Playtech, Microgaming e Cryptologic. In addition: “About the Software’s features” RNG is an open platform that offers Luckland a good level of customization options. Realtime Gaming distinctive feature is a very specific graphic footprint, as well as the development of exclusive gaming features. In terms for personnel we interact with, RNG hired new talents in the programming field, in web interaction sector and in the field of strategic analysis and offered us very effective applications. About “Real Time Gaming”: a. Speed: the games load faster, with a better performance than that of other platforms;
--------	---	--

		b. variety: wide choice of poker games, 3 and 5 reel slot machines, multi-line video slots, progressive jackpots; c. Realism: striking and photorealistic graphics for roulette, blackjack, craps; d. Dual-screen: it is possible to execute two games simultaneously, 'splitting' the screen; e. Mini games: very small windows are opened to follow more than one game at the same time; f. Welcome bonus: in its sector, RTG is famous to offer some of the highest welcome bonuses. Of course Luckland can freely decide which payouts to fix for every single promotion, according to its risk appetite; g. Technical support: automatic updates, support in marketing operations, total and accurate control on game speed; h. Safety: thanks to Technical Systems Testing, a verification process of the Random Number Generator, RTG software is "certified" to be reliable and it offers guarantees about players' winning probabilities. That's why it is worldwide accepted within every jurisdiction. Regarding the "variety of games offered" In the field of innovative and practical game solutions' design, RTG offers online casino and slot machines, all managed through a single platform. It's Real Time Gaming Software Casino package that has a great "in-bundle" back-end suite, a business device to create your online gaming platform easily. Because of that Luckland can easily check entries, exits, operations in progress through your online account, monitoring in real time all the players' stakes and the performances of the games offered. In this way, whether any technical problem or claim may occur the staff will immediately start working. The management has been made easier using advanced reporting devices that analyze the operations providing a database; such a database is important to address marketing strategies.
--	--	--

		Finally, as for the “RealTime Gaming software casino package”, Luckland Live game mode rooms are very graphically accurate, the game is fast and reliable.
	4. Which game providers are used?	Please, kindly see under our answer to question n.3 above (Where the topic was covered already).

	5. Are any games restricted to specific jurisdictions or player categories?	Yes, Luckland Group considers the Centrale Bank van Curaçao en Sint Maarten (CBCS) would Informative document about the state of affairs concerning European sanctions 1 and national sanctions of the Netherlands 2 This report covers the period from February 1- February 28, 2026, Luland updates the sanctions list screening until the last FATF Plenary of 11 June 2026. During this period, changes were made to the sanctions' regimes concerning Russia, Ukraine, Belarus, Zimbabwe, Iran. Luckland is committed to complying with targeted financial sanctions (as, which require the freezing of funds and assets of individuals and entities identified by the United Nations (UN) and European Union (EU) as being involved in terrorism or proliferation activities. Mechanisms are established to ensure compliance with Luckland Group's legal obligations. This includes, but is not limited to, the following: More precisely, in the event that a true match is discovered and confirmed, Luckland Group must immediately proceed with freezing the funds of the particular customer(s), in accordance with the Sanctions Ordinance, and must immediately file a report with the FIU. Once the true match is confirmed by the supervisory authority, Luckland Group shall terminate services and keep the frozen assets until further instruction from the supervisory authority, or otherwise, in light of tipping off considerations, follow instructions from the supervisory authority. a. Luckland Group shall comply with relevant sanctions decrees and regulations and monitor any and all amendments thereof and implement these without undue delay. b. Luckland Group shall perform ongoing sanctions screening on customers and also perform trigger-based sanctions screening of customers in the following scenarios: 1. At the moment of registration; 2. At the moment of withdrawal request; 3. At the moment of any request for change of personal details or payment methods. The updated FATF list, Luckland considers among others, includes the "Required Action" tab, which outlines the measures operators must implement, as well as the reason for geo-block.
--	--	---

		The updated Restricted Markets List for your review and implementation: Notwithstanding, a Curaçao gaming license does not, by itself, authorize operators to target all jurisdictions. Each market must be assessed under its own local laws, including gambling, licensing, sanctions, AML/CFT/CPF, advertising, payment, tax, consumer protection and responsible gaming requirements. 1. Operators remain responsible for conducting and documenting their own market due diligence before entering or continuing to service any jurisdiction. Where a market is prohibited, restricted, locally licensed, sanctioned, high-risk or uncertain, appropriate controls must be implemented, including where relevant geo-blocking, payment blocking, affiliate restrictions and marketing exclusions. 2. The attached list is provided as a practical reference only and is not exhaustive. Operators must continue to monitor legal and regulatory developments and should obtain local legal advice where required. 3. Please ensure that your websites, onboarding controls, payment flows, affiliate arrangements and marketing activities are aligned with the updated list. Where any listed or otherwise restricted market is currently being targeted or serviced, please conduct a documented review and take remedial action without delay.
	6. How does the operator ensure that only approved or permitted games are made available?	An operator must maintain at least one gaming server physically located in Curacao, all gaming software must be tested and certified by accredited independent testing laboratories. In addition under the Curacao Gaming Brief, in order to be made available the games they will play, prior to account creation, players must satisfy defined eligibility requirements, including age verification and jurisdictional restrictions. They are also required to provide accurate registration information and maintain responsible account usage.

P a y m e n t p o s s i b i l i t i e s	7. Which deposit methods are accepted?	Luckland is aware that some payment methods can also involve funding accounts using credit and debit cards, prepaid cards, checks, and cryptocurrency, followed by requests for payouts or inserting funds into gaming machines and immediately claiming those funds as credits. That is why it accepts different deposit methods depending on game (for instance for slots it accepts only, Mastercard, Amex, Instant bank transfer and Apple pay) and country and set strict limits: 1. Deposits: 500+ 2. Withdrawals: 2000 Besides, Luckland manages high risk country located PSPs methods allowing only cc or e-wallets processing. Please, note that withdrawals are subject to “AML/KYC verification”.
	8. Which withdrawal methods are available?	The same of deposit, as soon as they are verified
	9. Are fiat currencies, crypto-assets, vouchers, e-wallets, bank cards, bank transfers, or alternative payment methods used?	Mainly: e-wallets, bank transfers and bank cards, but also all the others depending on a risks based approach and local regulations.
	10. Which payment service providers are involved?	Postepay, Visa, Mastercard, Bank Wite, Ethereum, eZeewallet, Litecoin , (but in different high-risk jurisdictions, depending on the PSP risk /we could accept also cc and e-wallets only)
	11. Are there minimum and maximum deposit and withdrawal limits?	Deposits:500 Withdrawals 2000
	12. Are payment methods subject to verification before use?	YES
	13. Are deposits and withdrawals only permitted through accounts held in the player’s own name?	YES

	14. How are failed, reversed, or suspicious payments handled?	Luckland detects, halts, and reports all suspicious payments to the Financial Intelligence Unit (FIU Curaçao). Transactions flagged as unusual must be filed immediately via the goAML platform to prevent money laundering and terrorism financing. The main obligations for suspicious payments mandatory Reporting are that both shall be executed and, proposed transactions must be reported if they trigger objective or subjective indicators (e.g., sudden large deposits, erratic betting patterns, or attempting to use prohibited assets). No tipping off on any reversed, failed or suspicious is allowed. Luckland and staff are legally prohibited from informing a player that a Suspicious Transaction Report (STR) or Suspicious Activity Report (SAR) - (unusual), has been filed against them. Source of Funds (SOF), in such a case Luckland proactively trace the origins of suspicious wealth. If a transaction cannot be verified, Luckland initiate Enhanced Due Diligence (EDD) or refuses to process the payment.
B e t t i n g l i m i t s	15. What are the minimum and maximum bet amounts per game?	500
	16. Are limits different per game, provider, player category, or jurisdiction?	YES
	17. Are stake limits configurable by the player?	YES
	18. Are internal risk limits applied by the operator?	YES
	19. Are responsible gaming limits applied to deposits, stakes, losses, or session activity?	YES

	20. How are changes to betting limits approved and recorded?	At Luckland, Players must be able to access a detailed record of their betting and wagering history including limits change, timestamps of transactions from their player account of at least the last six months, without prejudice to retention periods required by other applicable laws and regulations. Longer periods of transactions may be requested from the operator and must be provided within 10 working days. If the operator can show that this timeframe is not reasonably achievable given the circumstances, Luckland is aware that the CGA may grant an extension for a period it deems appropriate. Players should be encouraged to regularly assess their gaming habits to determine whether their gambling remains within healthy limits by providing self-assessment tools that allow them to answer a series of questions designed to help identify potential problem gambling behaviours. These tools empower players to make informed decisions about their gambling activity.
P a y o u t s a n d w i n n i n g s	21. What payout percentages, odds, prize structures, or return-to-player rates apply?	For Payouts, it can also involve funding casino accounts using credit and debit cards, prepaid cards, followed by requests for payouts or inserting funds into gaming machines and immediately claiming those funds as credits. Hence this is considered on a case by case basis.
	22. Are payout rules displayed to players before participation?	Payouts are to be displayed to players before participation in any regulated gaming session/event. These rules must clearly outline: a. Prize structures, how the prize pool or odds are distributed among winners. b. Wagering requirements, any playthrough conditions or fees that apply to withdrawals. c. Entry limits: The amount staked compared to the potential return. Besides, we apply the specific regulatory requirements and display guidelines for that specific game

	23. How are winnings credited to player accounts?	Since, financial transactions do not refer to gambling transactions that include only casino chips or tokens. Winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions. That said, winnings from our online gaming are automatically credited to the Player's site account balance as soon as the bet settles. Once credited, he can leave the funds in your wallet to use for future wagers or request a withdrawal to his/her preferred bank or e-wallet. So, how the process works in practice: - Automatic Credit, the moment a game finishes or a bet is settled, the winning funds are added to your active account balance. - Withdrawal Requests, to move these funds into your personal bank or payment service, you must navigate to the platform's cashier/wallet section and submit a withdrawal request. - Verification & Processing, our Platforms typically require identity verification (KYC) to combat fraud before releasing funds. Processing times vary; e-wallets often take a few hours, while bank transfers and debit cards generally take 1 to 5 business days.
	24. Are jackpot, bonus, tournament, or promotional payouts handled differently?	It is handled on a case by case basis depending on the amounts and risk.
	25. Are there maximum payout limits?	It depends if multiple wagering is involved
	26. What happens if a game, system, or payment error affects a payout?	The "Malfunction Voids All Pays" clause is one of the most important and controversial rules in online gaming. It means that if a technical error occurs during a game, any winnings from that round can be cancelled, even if they appeared on your screen. This clause is extremely common and included in almost every casino's terms. However, it doesn't always apply in the same way. Licensed casinos are required to enforce it fairly and review each case carefully, while unregulated platforms may apply it more strictly. For players, this means a visible win is not always guaranteed if a system glitch is detected. For more, please see our uploaded policy: Information -Security-Policy-Luckland-Group-BV..pdf

	27. How are disputed payouts investigated?	At Luckland, payout disputes are investigated through a multi-step process involving internal audits by the operator, reviews by payment processors, and often independent or regulatory arbitration. The goal is to determine whether the rules were followed or if the transaction was fraudulent. The investigation process generally breaks down into these core stages: 1. Internal Audit by the Operator Before an issue is escalated to an outside authority, the gaming platform's internal risk and compliance teams investigate: Game Logs & Server States: The operator pulls exact server-side logs to verify whether a winning bet was officially recorded, if a glitch interrupted the session, or if bonus wagering requirements were met. Session & Account Data: Analysts review login timestamps, IP addresses, device identifiers, and geo-location data to verify if the account owner was the one who placed the bets. KYC (Know Your Customer) Check: The team verifies if the account was properly registered and that the player did not violate terms of service, such as operating duplicate accounts or using unauthorized software. 2. Payment Processor & Bank Review (Chargebacks) If the payout dispute stems from a player claiming an unauthorized deposit to their bank or credit card (a chargeback): Representment: The gaming operator submits a "package" of evidence to its acquiring bank. This usually includes transaction receipts, IP logs, and proof that the player accepted the terms of service. Card Network Ruling: The credit card issuer (e.g., Visa or Mastercard) evaluates the evidence from both the player and the merchant before making a final decision on who keeps the funds
--	---	---

S o f t w a r e u s e d i n t h e o p e r a t i o n	28. What platform software is used?	Ensure tracking runson "RNG software". Luckland tracks all unauthorized software deployed within the organization to reduce risk from unauthorized, unsupported, or outdated applications. Implementation Guidance: a. Maintain an inventory of all software used, including: o Gaming software platforms b. Operating systems c. Endpoint and server security tools d. Reporting, management, and compliance applications e. Jurisdiction ROM Version f. Document for each game software entry, where applicable, according to industry specific requirements g. Title and game variant h. Version and installation date i. Purpose and associated business function o Number of licenses or installations j. Review and update the software inventory bi-annually k. Gaming-specific consideration: game engines, and other components subject to regulatory oversight. This control maps to CIS 2.1 and supports ISO/IEC 27001:2022 control A.5.9. 1.9.4 Verify Software Support Status and Address Unsupported Applications Operators must verify that all installed software is currently supported by vendors and establish procedures to manage unsupported software.
	29. Which game aggregation, wallet, payment, KYC, AML, fraud monitoring, reporting, responsible gaming, CRM, and back-office systems are used?	Luckland has a proprietary solution the Risk Assessment Tool (RAT) which is required to be completed before the establishment of a relationship. This tool holds the integrated risk classifier of the applicant for business in relation to, KYC, AML, Fraud, RG and back end. All such forms are to be duly completed, signed off by the MLRO and filed in the respective customer file.
	30. Are systems proprietary or supplied by third parties?	Both

	31. Who maintains and updates the software?	Game software is maintained and updated by the game's development studio. Specific teams, including software engineers, Quality Assurance (QA) testers, and LiveOps (Live Operations) team, work together to fix bugs, balance mechanics, and release new content. Here is how the update process works behind the scenes: Software Engineers / Programmers, they write and rewrite the code, optimize performance, and build patches. QA Testers, they actively search for bugs, attempt to break the game, and verify that the developers' fixes actually work before public release. [1, 2] LiveOps Teams: Common in multiplayer and free-to-play games, these teams monitor servers and deploy dynamic, real-time events and seasonal content. Ultimately also the MLRO has 2nd level of control on it.
	32. How are software changes tested before release?	At Luckland, game software is maintained and updated by the game's development studio (e.g., Wikipedia Video Game Developer). Specific teams, including software engineers, Quality Assurance (QA) testers, and LiveOps (Live Operations) teams, work together to fix bugs, balance mechanics, and release new content. Here is how the update process works behind the scenes: Software Engineers / Programmers: They write and rewrite the code, optimize performance, and build patches. QA Testers, they actively search for bugs, attempt to break the game, and verify that the developers' fixes actually work before public release. [1, 2] LiveOps Teams, common in multiplayer and free-to-play games, these teams monitor servers and deploy dynamic, real-time events and seasonal content. Also the MLRO shall be vigilant and give the green-lights to the change.

	33. How are software versions documented?	At Luckland, gaming software versions are documented using a combination of numerical sequences, state indicators, and source control tags. They rely on a mix of developer-facing tracking (builds, commits) and player-facing conventions (semantic versioning, platforms) to establish a clear chronological and structural history of the game. 1. Common Versioning Schemes Semantic Versioning, a widespread 3-digit format written as Major.Minor.Patch (e.g., 1.4.2). Major: Incremented for massive, potentially save-breaking expansions or overhauls. Minor, incremented for compatible new features, content additions, or seasonal events. Patch, incremented for minor rebalances, bug fixes, or text fixes. Build/Changelist Numbers: Often used as a fourth number (e.g., 1.0.4.5218). The final digit represents the exact internal snapshot or commit hash from version control. Live-service games frequently tie this number directly to their internal code repository tools. Calendar Versioning (CalVer): Uses the date of release (e.g., 2026.04.1). This is occasionally used by indie studios during the "Alpha/Early Access" phase to easily distinguish daily or weekly testing builds. Stage Indicators: Alphanumeric suffixes are used to denote the software release cycle, such as .a(Alpha), .b (Beta), .rc (Release Candidate), or tag additions like -earlyaccess. 2. Internal Documentation & Tracking Version Control Systems (VCS), every change creates a unique, chronological snapshot. [Changelogs, written text files maintained by developers to communicate exactly what changed from the previous version (e.g., balance adjustments, known bugs).
--	--	---

	34. How are access rights to software systems controlled?	At Luckland, access rights to gaming software systems are primarily controlled through Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), and token-based authentication (like OAuth 2.0 and JWT). These methods restrict system access to developers, administrators, and players based on verified permissions. The main mechanisms include: Authentication (AuthN): Verifies who you are using identity providers, Multi-Factor Authentication (MFA), and Single Sign-On (SSO) to prevent unauthorized logins. Authorization determines what you can do. For developers, this restricts access to source code or production databases. For players, it verifies account subscriptions, entitlements, and region locks. Role-Based Access Control (RBAC), that assigns system permissions based on job roles or player tiers rather than individual users. Example: A "Community Manager" may have rights to ban users and edit forum posts, while a "Game Master" is restricted to in-game monitoring and player support. Attribute-Based Access Control (ABAC): Grants access dynamically by evaluating rules based on specific attributes (e.g., time of day, geographic location, or account age). Entitlement Systems, digital rights management (DRM) and launcher platforms (like Steam or Epic Games) check licenses to ensure the user has legally purchased or subscribed to the game before launching. Federated Identity: Allows users to log into games using external accounts while strictly sharing only necessary credentials rather than full passwords
--	--	--

O u t c o m e - d e t e r m i n i n g e l e m e n t s	35. Are outcomes determined by random number generators, live dealer results, sports results, player decisions, algorithms, or other mechanisms?	A mix of all. Please see more in detail our Security Policy mentioned above: Information-Security-Policy-Luckland-Group-BV..pdf
	36. Which systems or providers determine outcomes? .	In gaming outcomes are determined by a combination of Random Numbers generators (RNG) and internal game engines and Matchmaking/skill based Systems /SBMM. The specific systems that control your results depend on the type of game you are playing. Digital & Casino Gaming: Random Number Generators (RNG): In games of chance (slots, digital cards, roulette), an algorithm generates thousands of numbers per second. The exact fraction of a second you press "spin" or "deal" determines your result. [1] Provider & Regulation: Game studios (e.g., SOFTSWISS) design the math models, while independent testing labs (such as eCOGRA) audit the RNGs to ensure they are mathematically fair and truly random
	37. How is randomness tested and certified?	Via RNG testing, which includes software-based (pseudo-algorithmic) RNG's. Hardware RNG's and hybrid combination of both.
	38. Are RNG certificates available?	YES

	39. How are game rules, payables, odds, and outcome logic documented?	At Luckland, game rules and outgoing logic are typically documented using both player-facing manuals and developer-level technical documents. The documentation ensures a clear, shared understanding of how the mechanics function and how players interact with the system. Player-Facing Documentation: Game rules for physical or digital games are outlined in a formalized, structured manner. Standard practice follows a specific layout so players and judges can easily find information: Overview & Objective, defines the premise of the game and how a player wins. Components & Setup, lists all elements in the game and their initial placement. Sequence of Play, details step-by-step turn structure and outgoing actions. Glossary & Examples: Clarifies edge cases, definitions, and provides pictorial examples to prevent rule misinterpretation. Developer-Level Documentation: For software development, rules and outgoing logic (like processing game loops or network payouts) are broken down into technical specifications. These are documented via: Game Design Documents (GDD): The central "bible" created by designers that outlines the core concepts and mechanics of the game. Flowcharts & State Machines: Visual representations that track the flow of logic, detailing specific input triggers and how the game transitions from one state to the next. Pseudo-code & Logic Trees: Written out step-by-step programmatic logic mapping out conditionals and rules before it is written in actual code. Technical Architecture/Codebase Comments: Standard inline documentation in shared codebases ensures both client and server can predict and verify actions consistently
--	--	---

	40. How does the operator prevent manipulation of outcomes? How are incidents involving incorrect game outcomes handled?	Gaming incident handling manages unexpected disruptions or cyber attacks, minimizing downtime, revenue loss, and player frustration. The standard lifecycle consists of 5 primary steps: Preparation, Identification, Containment, Eradication/Recovery, and Post-Incident Review. The Luckland, 5-Step Incident Lifecycle: 1. Preparation: Establish a 24/7 incident response plan to ensure your live-ops, security, and compliance teams know exactly how to act under pressure. 2. Identification: Monitor servers and player telemetry to quickly detect anomalies, distinguishing between standard bugs and severe breaches. 3. Containment: Isolate compromised servers or lockout suspicious sessions to prevent the issue from spreading further into the player base. 4. Eradication and Recovery: Remove the root cause of the incident and restore standard game operations via safe backups. 5. Post-Incident Insights: Document the incident for audits and implement technical security improvements to prevent future occurrences
--	---	---

P e r i o d i c t e s t m e t h o d s f o r q u a l i t y m o n i t o r i	41. Which systems are tested periodically? 42.	Each of them
	43. 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?	YES
	44. How often are tests conducted?	In the gaming industry, vulnerability testing is an ongoing cycle rather than a one-time event. Security teams rely on a tiered schedule, so as at Luckland. a. Continuous / Daily: Automated vulnerability scans run constantly behind the scenes to track new threats in live-service environments. b. Weekly to Monthly: In-depth vulnerability assessments and reports are processed to review and patch code vulnerabilities. c. Quarterly: Comprehensive baseline penetration tests and audits. d. On-Demand: Mandatory tests after any significant update, patch, infrastructure change, or new release
	45. Who performs the tests: internal staff, external auditors, labs, suppliers, or consultants?	A Hybrid mix of all.
	46. How are test results documented?	A testing documentation results as follows, considering if "a game works as intended". Test Cases, Step-by-step instructions with expected results (e.g., verifying that pressing the "Jump" key results in the character jumping). Testers check each case and mark it as Passed, Failed, or Blocked. Defect Logs: When a test fails, a bug is logged in specialized tracking software like Jira. These reports include the unique Test Case ID, the game build version, the platform, the severity of the bug, and exact steps to reproduce it. Visual Evidence, screenshots or screen recordings are frequently attached to bug reports to help developers instantly visualize the issue

n g	47. How are deficiencies corrected?	IN gaming, "deficiencies" generally refer to three distinct categories: software bugs/performance issues, gameplay imbalances (e.g., overpowered weapons), or physical/accessibility limitations (e.g., colorblindness). Developers and players use specific tools and strategies to correct each type. How Deficiencies are Corrected at Lucland: 1. Software & Performance Bugs For glitches, crashes, and performance drops, developers typically rely on the following methods: Patches and Hotfixes: Developers rewrite or modify the source code to fix bugs and upload the updated data to patching services. Modern games routinely receive downloadable updates that fix problems ranging from faulty physics to memory leaks. Player Reporting: Players assist in the correction process by submitting bug reports through official game websites or using automated feedback tools built directly into the game's launcher. 2. Gameplay Imbalances When certain characters, items, or strategies become overwhelmingly superior, they ruin game variety and player choice. To correct this, developers utilize: Buffs and Nerfs: Developers adjust numerical values—such as weapon damage, character health, or ability cooldowns—to bring all playable options back in line with one another. Decreasing utility is known as a "nerf," while increasing utility is a "buff". Playtesting and Feedback: Balancing heavily relies on Quality Assurance (QA) teams and live-testing data from the player community to prioritize what needs adjustment in upcoming patches. 3. Visual & Accessibility Deficiencies If players have conditions like color vision deficiency (color blindness), which make distinguishing vital visual information difficult, modern game studios correct this through accessibility options.
--------	-------------------------------------	---

		a. Customizable UI Colors, developers add settings that allow users to alter the colors of specific essential indicator, like enemy team colors or health bars, without changing the rest of the game's aesthetic palette. b. Secondary Cues, games introduce redundant visual or auditory clues, such as pattern matching, icons, or directional audio, to help all players understand in-game states
	48. Who verifies that corrective actions have been completed?	At Lukland, depending on whether you mean fixing a bug in the game or legal/policy issue, the verification responsibility falls to different professionals. It may also involve the management and Oversight Board when a Corrective and preventive action plan is submitted.

S t o r a g e o f p l a y e r s , p e r s o n a l d a t a a n d o	49. What personal data is collected from players?	At Luckland, Personal Data shall be collected only where necessary for clearly defined and lawful purposes, including player account registration and verification, provision of gaming services, fraud prevention, and regulatory compliance (including AML/ CFT and responsible gaming obligations). At the point of collecting, the Company shall inform individuals of the purpose and legal basis for processing, collect only the minimum data required for stated purpose, and avoid the collection of special categories of data unless a lawful exception applies. Special categories of Personal Data, such as health information or political views are subject to stricter protection. These may only be processed if: • The player has given explicit consent. • The processing is required by law (e.g., employment obligations). • It is necessary to protect the player's vital interests. • The data has been made public by the player. • It is required for legal claims, public health, or other specific grounds.
---	---	--

t h e r e d e t a i l s	50. What identification, verification, contact, financial, gaming, technical, and communication data is stored?	Identification: 1. Valid full name 2. Date an place o Birth 3. Nationaliy 4. Identity Reference number,where available 5. Residential address Verification: 6. Valid Unexpired passport; or 7. Valid, Unexpired national; or other government issued identity card, or 8. Valid Unexpired Residence card; or 9. Valis Car License *And documents less than 3 months old and address of applicant in a clear manner. 10. Utility Bill 11. Bank Statement or Bank Reference Letter 12. Correspondence from a government authority , department or agency 13. Any Identification Document listed above, where a clear indication of the address provided 14. Official Conduct Certificate; or 15. Other government issued document not mentioned above 16. Use of electronic data provider or electronic identification and verification solutions
--	---	---

	51. Where is the data stored? Which systems or databases contain player data?	KYC (Know Your Customer) data is typically stored in secure, encrypted databases maintained by the specific organization you are onboarding with (e.g., banks or crypto exchanges). At Luckland, depending on the region and industry, this information may also be held by specialized third-party verification providers, global KYC registries, or centralized government databases Players i Curacao are mainly captured in our CRM and RNG. For other detailed information see our:comprehensive:Information-Security-Policy-Luckland-Group-BV..pdf
	52. Who has access to the data?	In the gaming industry, multiple entities access and utilize your data, ranging from the creators of the game to third-party services and other players: Game Developers and Publishers: Studios collect and process telemetry, hardware stats, and in-game behavior. This data is used to debug issues, balance gameplay, and plan future updates. However the main ones are: 1. The data Protection officer (DPO) and MLRO can have access but are strictly limited to their mutual roles. 2. Platform Holders, companies operating your gaming ecosystem have access to your account details, purchase history, and friend lists. 3. Third-Party Analytics & Cloud Services, middleware providers like Unity Analytics or AWS host game servers and aggregate user data. 4. Upon consent, Advertisers and Marketing Partners, Free-to-play and mobile games frequently share profile and behavioral data with ad networks to deliver targeted advertisements

	53. How is access controlled and logged?	.At Luckland, data access is primarily controlled via server-authoritative architectures and role-based access controls (RBAC), and is monitored through real-time telemetry and centralized logging. The approach balances high-performance needs during active gameplay with strict security for persistent user data. 1. Data Access Control Game developers prevent unauthorized manipulation and secure sensitive user information using specific protocols: Server-Authoritative Design: For multiplayer games, the central server acts as the absolute "source of truth." Clients (the players' devices) cannot directly modify databases. They only send inputs, which the server validates before taking game-state actions like deducting currency or confirming damage. 2. Database Segregation: Studios typically use separate database schemas or completely different server systems to separate active, dynamic game data (e.g., in-game inventory, character stats) from highly sensitive corporate and marketing data (e.g., emails, payment information). Principle of Least Privilege: Internal staff and automated systems are only granted the specific data access necessary for their tasks. Administrative changes require Multi-Factor Authentication (MFA) and strict role authorizations. 3. Logging & Monitoring Studios maintain tamper-proof, time-stamped logs to track gameplay health, detect cheats, and maintain regulatory compliance (such as GDPR): [1, 2, 3] Game Telemetry & Event Logs: Servers capture and store logs recording session details, connection timestamps, match IDs, and transaction details linked to randomized player IDs. 4. Security & Anti-Cheat Logging: Systems track unauthorized client modifications, abnormal actions, and repeated password reset attempts, which are actively monitored in near-real-time to flag fraudulent activity. [1, 2, 3]
--	--	---

		Data Retention: While general gameplay telemetry might only be temporarily cached, security logs are often kept for months, and billing/financial records are typically retained for several years depending on legal requirements
--	--	--

	54. How is data encrypted or otherwise protected?	At Luckland, access to player personal data and gaming records is strictly limited to authorized personnel whose duties require such access. Access to systems and data shall be granted on a “need-to-know” and “least privilege” basis. Only the Company-approved devices that meet defined security standards may be used to access systems containing player data, gaming records, or financial information. The use of personal or unmanaged devices for such access is prohibited unless expressly authorized and subject to equivalent security controls. All Company-approved endpoints used to access sensitive systems shall be subject to the following minimum-security requirements: a. Encryption: Devices must use full-disk encryption or equivalent safeguards to protect data at rest and in transit. b. Secure Configuration: Endpoints shall be configured in accordance with Company security standards, including timely installation of operating system and application security updates and the disabling of unnecessary services and software. c. Antivirus/ Endpoint Detection and Response: Approved antivirus and/ or EDR solutions must be installed, active, and regularly updated on all endpoints accessing the Company systems. d. Remote Access Controls: Remote access to Company systems shall only be permitted through approved secure channels and is subject to strong authentication controls, including multi-factor authentication (MFA). e. Prohibited Uses: Endpoints used for Company operations must not be used for unauthorized software installation, insecure file sharing, or activities that may compromise the confidentiality, integrity, or availability of Company data. Role-based access control shall be implemented for all systems handling player or financial data. MFA is mandatory for all privileged accounts and remote access. Privileged accounts must be separately monitored, logged, and reviewed quarterly
--	--	--

		by the Compliance Officer and IT teams. Access rights must be revoked promptly upon termination of employment or engagement. Accounts of termination users shall be disabled within 24 hours of departure or immediately where risk is identified. The Company shall further: f. Maintain access logs of all staff interactions with personal data and critical gaming and financial systems. g. Require confidentiality agreements and data protection obligations for all employees and contractors with access to sensitive information. h. Prohibit disclosure of personal data to third parties except: 1. As required for regulatory compliance (e.g., CGA, AML/ CFT reporting) or; 2. Where mandated by law, with proper documentation. Any suspected compromise of an endpoint or unauthorized access to systems shall be treated as a security incident and handled in accordance with the Company incident Response Plan
	55. What retention periods apply?	Where Personal Data must be retained beyond its primary operational use for legal, regulatory, or audit purposes, it shall be archived securely. Archived data shall be segregated from active systems, subject to restricted access controls, protected against unauthorized modification or deletion, and retained only for as long as legally required. From 5 up to 7 years depending on ANL needs (i.e. ongoing investigations)

	56. How are data correction, deletion, or access requests handled?	Players (data subjects) have several rights regarding their personal data: 1. Right to be informed: Players must be told how their data is collected, used, shared, and retained in a clear and accessible way. 2. Right of access: Players can request a copy of their personal data. Responses must be provided free of charge (except in abusive cases) and within one month, unless extended in accordance with Data Protection Laws. 3. Right to rectification: Incorrect or incomplete data must be corrected promptly. 4. Right to erasure ("right to be forgotten"): In certain circumstances, players can request deletion of their data. 5. Right to restrict processing: Players can request that their data be stored but not actively processed. 6. Right to data portability: Players can request their data in a commonly used, machine-readable format. 7. Right to object: Players may object to processing based on legitimate interests or direct marketing. 8. Rights related to automated decision making: Players have the right not to subject to decisions made solely by automated processes without human oversight, except where allowed by law or explicit consent. 10 5.6 Communication Channels for Data Subjects The Company shall ensure that clear and accessible communication channels are available for players and other data subjects to contact the DPO regarding data protection matters. These channels shall include: 1. Contact details published in the Company's Privacy Notice; 2. A dedicated email address or other appropriate means of; Communication; 3. Procedures for handling and responding to data subject requests and complaints in a timely manner. The DPO shall oversee the handling of data subject requests, including requests for access rectification, erasure, restriction, or objection to processing.
--	---	---

	57. How is data protected against unauthorized access, loss, alteration, or disclosure?	The Company shall maintain a documented Incident Response Plan covering: a. Detection: All staff must immediately report suspected security incidents. B. Assessment: The Incident Response Team (IRT) shall classify incidents by severity. C. Containment and Eradication: Immediate measures must be taken to prevent further damage. D. Notification: Regulatory reporting obligations (e.g., CGA, FIU, affected players) must be fulfilled within prescribed timelines. E. Recovery: Systems must be restored from secure backups. F. Post-Incident Review: Root cause analysis and corrective actions shall be documented. Regular incident response drills shall be conducted to test readiness for data recovery.

V i s u a l e l e m e n t s s h o w n t o p l a y e r s	58. What websites, domains, mobile applications, or software interfaces are used?	They are fully displayed below: For the Websites www.casinomidas.com www.jackmillion.com www.spinsamba.com www.spingrande.com For the Apps/Software: https://casinomidas.com https://jackmillion.com https://spinsamba.com https://spingrande.com
	59. 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?	They are fully displayed in here (as per above): www.casinomidas.com www.jackmillion.com www.spinsamba.com www.spingrande.com

	60. Are visual elements consistent across desktop and mobile versions?	In multi-platform games as at Luckland, core art style, branding, and color schemes are usually consistent across desktop and mobile. However, technical limitations and varied input methods often require significant differences in graphical fidelity, user interfaces (UI), and layout spacing. Specific differences between platforms include: Graphics and Performance: Desktop versions generally feature higher-resolution textures, complex shaders, advanced lighting, and higher frame rates. Mobile devices typically use lower polygon counts and scaled-down effects to preserve battery and prevent overheating. User Interface (UI) and Layout, desktop displays allow for rich, multi-layered menus and information displays since the screen size is larger. Mobile UIs are often minimalist and feature larger, thumb-friendly buttons to avoid cluttering the smaller touchscreen area. Asset Density, games built natively for PC may have environmental elements or text boxes that are scaled down or condensed on mobile devices to prevent the screen from looking cluttered. Rendering Architecture: Due to hardware differences, visual features that run well on desktop, like certain post-processing effects, might be incredibly expensive (and cause lag) on mobile. Most game developers strive to maintain a cohesive visual identity so players get a familiar experience, though the exact visual presentation adjusts to what the hardware can smoothly display
	61. Are legally required notices clearly visible?	YES
	62. Are game rules, risks, odds, limits, and responsible gaming tools easy to find?	YES

	63. How are changes to visual elements reviewed and approved?	Ultimately by the Responsible Gambling Officer as 2nd line of defence. However, visual changes in video games are primarily reviewed and approved by the game's Art Director and Creative Director, alongside Lead Artists. They ensure changes align with the project's overarching style guide. The exact hierarchy and pipeline for this approval vary based on the studio's size: Art Director (AD), the highest visual authority. They dictate the game's aesthetic and give final sign-off on major visual assets, character designs, and environmental overhauls. Creative Director, focuses on the overarching vision and gameplay experience, ensuring the visuals make sense within the game's lore and mechanics. Lead Artists: Manage the day-to-day work of the art team. They review in-progress textures, 3D models, and animations before passing them up to the AD. Technical Artists / Quality Assurance (QA), ensure the approved visual changes do not break performance, frame rates, or engine compatibility. Publishers & Licensees (if applicable): If the studio is working with a major IP (e.g., Marvel, Disney), external brand managers or producers must approve visual changes to ensure they respect corporate guidelines. Lucklandi is responsible for materials (including visual elements) provided to affiliates, representatives, sponsorships, ambassadors, social media influencers, including wordings and visual representations, where the influencers actions and/or statements are paid placement or advertisement. The operator must make any contracted third-party aware of their Responsible Gaming policy and require them to adhere to it. Responsible Gaming Messaging, all advertising must include a clearly visible responsible gaming message or slogan.
--	--	---

T e c h n i c a l m e a s u r e s t o p r e v e n t b a n n e d p	64. Which categories of banned or prohibited persons are blocked?	Luckland excludes a player as a high-risk intervention measure if: a. The player displays problematic gambling behaviour. b. The player attempts or engages in criminal activities through the operator's platform. c. Operators may not exclude players solely on the basis of the amount of their winnings. In addition, according to Article 1.4(d) of the LOK, it is prohibited for Luckland to allow a minor the opportunity to participate in games of chance. Operators must therefore implement rigorous age verification processes to ensure that all participants are of legal gambling age. During the account registration process, the operator must verify that the player is not a minor. This begins with self-attestation, where the player is required to enter their date of birth and confirm they are over 18 by selecting a designated checkbox and additional checks must be carried out to gain sufficient certainty that the individual is not a minor. If at any point, notwithstanding the checks put in place, the luckland becomes aware that the player is a minor, the account must be closed immediately. The civil law implications of this action must be considered. These may include the obligation to refund all deposits made by the player and the forfeiture of any winnings. The operator must clearly communicate the reason for the account closure to the minor. besides, regardless of the above, proof of age document submission and checks are subject to the CGA's Know Your Customer and AML policies and should at a minimum include a government-issued valid ID check (such as a passport, national ID, or driver's license) on reaching specified thresholds and in any case prior to first withdrawal. Secondary verification methods such as electronic verification systems, payment validation, third party or government database checks, selfie verification, may be undertaken by the operator at its own discretion, but do not supersede the government-issued document requirement.
---	---	---

e r s o n s f r o m p l a y i n g		Operators must maintain records of all age verification processes and their outcomes. These records must be made available for regulatory review. Operator-initiated exclusions must be formally documented, and records must be kept for at least five years. The CGA may request these records at any time.
---	--	---

	65. How does the operator identify banned persons during registration, login, deposit, or gameplay?	Especially for minors, Luckland to further prevent underage gambling, the operator is advised to remind adults that they should take precautions when sharing devices with minors - such as safeguarding usernames, passwords, and payment details. Additionally, we consider links to third-party software that can help restrict access to gambling websites. While there are myriad options available globally, the following third-party tools (some paid, some free) are examples that are available for website blocking and gambling site blocking in particular: BetBlocker – betblocker.org GamBlock – gamblock.com Gamban – gamban.com Luckland, identifies banned players using a combination of automated software and physical surveillance. The exact method depends on whether the platform is a digital game, an online sportsbook, or a physical casino, using tools ranging from hardware bans to facial recognition. a. Online Video Games Hardware ID (HWID) Bans, developers track the physical components of a banned player's computer (e.g., motherboard, GPU, or network card) and blacklist them. Even if the player creates a new account, the game's anti-cheat engine identifies the restricted hardware. b. IP Address Tracking, operators log IP addresses to block connections from known cheaters or ban-evaders. c. Behavioral Analytics, advanced anti-cheat software utilizes machine learning to analyze gameplay statistics and player inputs in real-time. If a player exhibits machine-like aim, impossible reaction times, or compromised input patterns, their profile is flagged for review. Please,for an additional explanation see answer to question 64, above.
--	--	--

	66. Are exclusion lists, self-exclusion databases, age verification systems, sanctions checks, duplicate account checks, geolocation tools, identity verification tools, or device/IP checks used?	YES, It get blockedase see answer to question 65 for further details
	67. How often are checks performed?	At least every twelve months but, as a matter of fact more often and upon need. Just for the sake of major examples: a. Close to the period chosen for self-exclusion and cool-off ending, to possibly re-perform KYC; b. At same frequency of Sanctions Lists release and Quarterly as depending on FATF's Public Statements (Plenaries Calendar), to adjourn the prohibited countries and halt their residents from registering/playing; c. Sudden hits on co-owned accounts at onboarding and during the business relationship; d. New alerts on banned IP address e. New regulation requiring a licence in a certain country previously supported from Curacao etc.
	68. What happens if a banned person attempts to register or play?	1. It gets blocked and rejected, the MLRO evaluates if, a subjective indicator based, unusual transaction shall be reported.

	69. Are accounts suspended automatically or manually?	This is Hybrid, it can be manual if upon decision of the MLRO, RG Officer or Senior Management. Hence, large part, Luckland identifies banned players using a combination of automated software and physical surveillance. The exact method depends on whether the platform is a digital game, an online casino, etc. , using tools ranging from hardware bans to "facial recognition. Online Video Games Hardware ID (HWID) Bans: Developers track the physical components of a banned player's computer (e.g., motherboard, GPU, or network card) and blacklist them. Even if the player creates a new account, the game's anti-cheat engine identifies the restricted hardware at registration.; IP Address Tracking: Operators log IP addresses to block connections from known cheaters or ban-evaders at registration; Behavioral Analytics: Advanced anti-cheat software utilizes machine learning to analyze gameplay statistics and player inputs in real-time. If a player exhibits machine-like aim, impossible reaction times, or compromised input patterns, their profile is flagged for review during the onboarding stage
--	--	--

	70. How are attempted breaches recorded and reported internally?	At Luckland, all data breaches must be reported internally to the Board and the Compliance Officer as soon as possible. Breaches affecting personal data will be reported to the Curaçao Gaming Authority within 24 hours, with a full incident report including: nature of the breach, data affected, immediate actions taken and planned corrective measures. Where required by GDPR, affected players will also be notified. All breaches are logged and followed up with corrective actions. Further specific examples related to AML, sanctions, RG etc. In certain circumstances and up to how broader the meaning of “breach” is, the time of recording can depend, for example for Players identified as exhibiting at-risk behaviour after being informed of the Responsible Gaming tools available, such as deposit limits, cooling off, and self-exclusion options (duly recorded in the interaction and in or site/T&C); Luckland follows a clear escalation protocol where appropriate, which may include: a. Applying mandatory deposit limits to the player’s account (recorded in the back end and in RG tools); b. Temporarily suspending the account pending further assessment (recorded in the back end and in RG tools); c. Permanently excluding the player in cases of severe or persistent risk (block recorded in the front-end). However, under no circumstances may Luckland use Responsible Gaming measures as a pretext to prevent or delay legitimate player withdrawals. Any misuse of protective interventions for financial gain will be considered a breach of licence conditions (recorded in the relevant log and reported if needed).
--	---	--

T e c h n i c a l i n f r a s t r u c t u r e d i a g r a m	71. Does the manual include a clear diagram of the platform architecture?	YES - for details please see Luckland' upload in CGA Portal : Information-Security-Policy-Luckland-Group-BV..pdf
	72. 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?	YES - as per above
	73. Does it identify which systems are critical to the operation?	YES - as per above
	74. Does it show where player data, transaction data, and gaming data are stored?	YES - as per above
	75. Does it show data flows between systems?	YES - as per above
	76. Does it identify system owners or responsible parties?	YES - as per above

R e s t o r a t i o n p o s s i b il it i e s i n t e c h n i c a l e	77. What types of emergency situations are covered?	Luckland, shall define and maintain appropriate recovery objectives based on system criticality: a.Recovery Time Objective (RTO): The maximum acceptable time to restore critical systems following a disruption shall be defined and aligned with business and regulatory needs. For core gaming and player account systems, the target RTO shall be within a commercially reasonable timeframe (e.g., with 24 hours or less, subject to system classification); b. Recovery Point Objective (RPO): The maximum acceptable data loss in the event of an incident shall be defined and minimized for critical systems. For player and transaction data, the target RPO shall not exceed one business day and shall reflect the frequency of backups performed. RTO and RPO targets shall be reviewed periodically and tested as part of the disaster recovery and restoration exercises, c.Encryption and Data Security All player personal data, financial information and gaming records shall be encrypted. Encryption keys shall be managed securely with restricted access and regular rotation. Applications and systems are subject to secure coding standards, vulnerability scanning and periodic penetration testing.
--	---	--

m e r g e n c i e s	78. Are server failure, cyberattack, data loss, payment outage, game provider outage, platform outage, network failure, database corruption, and disaster recovery scenarios addressed?	Luckland is prepared to recover data and restore systems in the event of a cyber incident, hardware failure, or data corruption. A structured backup and recovery strategy is vital to business continuity and regulatory compliance. These controls align with CIS Control 11 and support ISO/IEC 27001:2022 control A.8.13. 1.18.1 Document the Data Recovery Strategy Luckland defines a comprehensive data recovery process, including backup planning, priority systems, and data integrity assurance. Implementation Guidance: a. Identifies which data types and systems require backup, with emphasis on critical gaming operations. b. Document the procedures for data backup, storage, and recovery testing c. Includes recovery point objectives (RPOs) and recovery time objectives (RTOs) d. Defines security measures for backup data, including access restrictions and encryption e. Reviews frequency, annually or when major systems or regulations change. f. Gaming-specific consideration: Ensure that gaming transaction data, configuration files, and player activity logs are included and protected in backups. This control maps to CIS 11.1 and supports ISO/IEC 27001:2022 control A.8.13. 1.18.2
--	--	---

	79. What backup procedures are in place?	Automate Backups and Enforce Isolation and Protection Operators must perform automated backups and ensure that backup data is adequately protected, isolated from production systems, and readily restorable. Implementation Guidance: a. Automate backups for systems handling sensitive or regulated data. b. Perform backups at a minimum weekly frequency; increase frequency for high risk or high-volume systems. c. Use offline, off-site, or immutable storage where feasible to prevent tampering or ransomware-related corruption. d. The Company shall maintain a documented Incident Response Plan covering: 1. Detection,all staff must immediately report suspected security incidents. • Assessment: The Incident Response Team (IRT) shall classify incidents by severity. 2. Containment and Eradication,immediate measures must be taken to prevent further damage. 3. Notification,Regulatory reporting obligations (e.g., CGA, FIU, affected players) must be fulfilled within prescribed timelines. 4. Recovery,systems must be restored from secure backups. 5. Post-Incident Review: Root cause analysis and corrective actions shall be documented.
	80. How often are backups made?	Gaming transaction logs and financial data may require daily or real-time backups to meet regulatory retention requirements and avoid data loss. In addition,Regular incident response drills shall be conducted to test readiness.

	81. Where are backups stored?	In principle, as a gaming operator licensed in Curaçao Luckland stores its core transaction logs, RNG systems, and player databases on physical servers located directly within the jurisdiction, typically in Tier-IV/Tier-III certified local data centers. In substance, post-incident, backup data must be restored and maintained in accordance with stringent disaster recovery and data localization mandates. Under the National Ordinance on Games of Chance (LOK) enforced by the Curaçao Gaming Authority (CGA), the storage and post-incident restoration of operator backup data must adhere to strict parameters, we observe: 1. In-Jurisdiction Localization, both primary operational databases and secondary data backups must reside on hardware within Curaçao to maintain data sovereignty and regulatory oversight; 2. Approved Infrastructure: Operators typically utilize specialized providers within certified local facilities, such as Blue NAP Americas (which serves also as the primary government-mandated infrastructure for backup systems); 3. Continent 8 Technologies; 4. Regulatory Compliance, following any data loss incident, operators must restore their backups to meet maximum Recovery Time; Objectives (RTO) and Recovery Point Objectives (RPO) apply if custom to gaming, ensuring all player balances, transactions, and AML records are kept in their integrity and are verifiable; 5. Cloud Replication Exclusions, while frontend web delivery and a number of auxiliary cloud components can operate globally, the master data nodes and backups must be housed domestically in Curaçao so the CGA can seamlessly conduct real-time compliance audits
--	-------------------------------	---

	82. What recovery time objectives and recovery point objectives apply?	Being Licensed by CGA, which does not prescribe fixed, universal Recovery Time Objectives (RTO) or Recovery Point Objectives (RPO), Luckland can follow the requirement to all licensed operators to formally establish, document, and test their own RTOs and RPOs based on the specific criticality of their systems and a Business Impact Analysis (BIA). Particularly, the CGA Information Security Framework Requirements state: a. Under the CGA's updated regulatory requirements, operators must comply with the Center for Internet Security (CIS) Controls; b. Implementation Group 1 (IG1) as the mandatory baseline; c. For disaster recovery and backups, operators must adhere to strict guidelines: 1. RTO and RPO Definition, operators must define RTOs and RPOs for all critical systems, ensuring they are suitable for a "gaming environment", 2. Data Criticality: Gaming transaction data, configuration files, and player activity logs must be included in the backup and recovery scope Automated Backups: Automated backups must be performed regularly, and this backup data must be isolated from production systems and encrypted. [1] Incident Reporting Hard Deadlines Along with establishing recovery objectives, the CGA introduced strict incident notification mandates. Licensees are required to notify the CGA without undue delay, and in any event within 24 hours of any security incident that compromises gaming integrity, affects player funds, or disrupts system availability
--	---	--

	83. Who is responsible for activating recovery procedures?	At Luckland, incident recovery procedures for data loss, service outages, and cyber breaches are activated by the Incident Response Team (IRT) or CSIRT (Computer Security Incident Response Team). This is coordinated by the Incident Response Manager, working alongside IT directors and project managers. A structured, cross-functional group initiates these protocols during a crisis: Incident Response Manager, assesses the severity of the incident, determines the scope of the emergency within 24 hours, and officially activates the company's recovery playbooks. Security Analysts and IT Ops, isolate the affected environments, verify the data backups, and execute the restoration of servers and player databases. Ops and Community Managers manage public outrage by pushing real-time status updates and player compensations through support channels and social media. Legal & Privacy Officers: Handle regulatory compliance, such as mandatory 72-hour reporting for data breaches (e.g., under the GDPR)
	84. How are players informed during service interruptions?	Luckland communicates game interruptions (such as downtime or server issues) to players in a proactive and clear way, in accordance with the National Ordinance on Games of Chance (LOK). In so doing, it adheres to CGA standards for managing and communicating system issues: 1. In-Platform Notifications, in case of unforeseen downtimes, we normally employ site-wide pop-ups, banner alerts, or maintenance landing pages; 2. Preemptive Communication, in case of scheduled maintenance, as per CGA's requirements about platform transparency, our Players are to be notified well in advance, detailing expected downtime; 3. Email and SMS, our Players are often notified directly through their registered communication channels (email or SMS) regarding longer-duration outages or account-specific impacts; 4. Incident Reports, as per the updated LOK framework, Luckland must report major system incidents through the Curaçao Gaming Authority Portal. What happens to your active game?

	85. How are unfinished games, pending bets, deposits, withdrawals, and balances handled after restoration?	Depending on the CGA-approved Terms and Conditions (T&Cs), affected game rounds are typically either voided with the wager refunded, or the game state is saved so it can be completed once service resumes. Besides, Luckland respects fair play and system integrity. If a game or transaction is interrupted while in progress due to a server failure, we investigate internally using the logs. If a disruption leads to a dispute that the our customer dedicated Departments can not resolve, players can escalate the issue to an independent, CGA-certified Alternative Dispute Resolution (ADR) entity. The ADR is listed in our ADR partners Terms and Conditions.
--	---	---

R e s p o n s i b l e g a m i n g p l e m e n t a t i o n	86. What responsible gaming policy applies?	The new version (compared to the one uploaded in the CGA portal, at present) is in progress to receive the instructions of the CGA, issued in April 2026, in their fullness).
	87. 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 license 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.

	88. 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 is subject to a 24-hour waiting period before implementation. 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 license. 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.
--	---	---

	89. 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.
	90. 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.

	91. 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.
	92. 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 license, 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.

	93. 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 organization. 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, Luckland believes that: Gambling should be a form of entertainment, not a way to make money.
--	---	---

		Players should always be in control of their time and spending. Vulnerable individuals, including minors, must be protected from the harms associated with gambling. Support should be easily accessible to those who need help with gambling-related issues. Transparency, integrity, and player well-being are fundamental to our operations. 2. Prevention of Underage Gambling Luckland has a zero-tolerance policy toward underage gambling. Our platform is available only to individuals who are at least 18 years old or who have reached the legal age in their jurisdiction, whichever is higher. We use electronic verification tools to confirm players' age and identity. Accounts suspected of being used by minors are immediately suspended, and any winnings are forfeited. 3. Player Protection Tools We offer several tools to help players manage their gaming activity: a. Deposit limits b. Loss limits c. Bet limits d. Session duration limits e. Reality checks f. Temporary breaks / Cooling-off periods Self-exclusion (at a specific given timing).
--	--	---

		As anticipated, Luckland 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. In essence the Tools provided are: - Self-exclusion (email/chat - 24/7) - Deposit limits - Cooling-off periods - Age verification (18+ enforcement) Behavioural monitoring via a specific algorithm and interaction with players identifies risky gambling patterns. For any Problem Gaming our players can contact our dedicated Support Center.
--	--	---

G e n e r a l T e r m s a n d C o n d i t i o n s	94. What is the current version number and date of the Terms and Conditions?	16 June 2026
	95. Are the Terms and Conditions included in full or attached as an annex?	Attached as an Annex, please see attached link: https://media.luckylandcasino.com/vgwholdings89e8-vgw-prod-817c/media/260616_POL_LLC_TCs_6-0.pdf
	96. Do they match the version published on the website or application?	Terms and Conditions (T&C) or End User License Agreements (EULAs) at Luckland are universally published in both places. They are integrated directly into the application (during installation or account creation) to enforce legal consent, and they are mirrored on the publisher's website for easy review. Where to find them: a. On the Application / Game Client: You are prompted to agree to these terms when you first launch the game, create an account, or install a major update. You can also typically find them in the game's Settings, Options, or About menus. b. On the Website: Publishers host permanent, updated versions of their T&Cs on their official domains, usually found in the footer of the page or in a dedicated "Legal" or "Support" section. c. On Digital Storefronts host links to both the game publisher's terms and the store's own user agreements
	97. How are updates to the Terms and Conditions approved?	Any updates of the terms and conditions of an online gambling operator must be approved by the Curaçao Gaming Authority (CGA). Precisely, under the new regulatory framework (LOK), the authority requires that the texts be clear and transparent and include specific clauses regarding: a. Account closure procedures a. Management of inactive accounts b. Rules for payments and refunds [1] All updates and final versions must be uploaded and validated via the official CGA portal.

	98. How are players notified of material changes?	Players are informed by Luckland of changes to terms and conditions via direct email notifications or pop-up alerts upon logging in. Under the regulatory framework (LOK) introduced by the regulator, operators are required to clearly highlight changes, provide previous versions upon request, and obtain renewed explicit acceptance. Communication methods include: Email: Gaming sites send notifications to the email address associated with the player's account, specifying the date the new rules take effect. Profile alerts: A banner or pop-up appears upon login, requiring the player to review the updates and click "Accept" to continue using the platform. Change history: Operators must ensure that updated versions of the terms remain accessible on all platforms at all times and provide previous versions upon a player's request.
	99. How is player acceptance recorded?	Registration of System Logs: Dealers keep digital traces (log), date and time when the user clicked on the confirmation button ("Register"), creating irrefutable proof of acceptance in case of litigation. Besides, referring also to the above questions 96 and 97, please note that: Acceptance of the Terms and Conditions (T&Cs) by a player is mainly is recorded through the express consent during registration and the execution of the contract (e.g. making the first play or the first deposit). The key steps through which the registration manifests and is proven include: a. Acceptance flag (Checkbox): The player must tick a non-pre-filled box during the creation of the game account, stating that he has read, understood and accepted the terms. b. Affixing a contractual link: This flag is always accompanied by a clickable textual reference to the complete document of the Terms and Conditions and the privacy rules. c. Account activation and first access: The completion of the opening of the game account, followed by authentication through credentials, perfects the contractual bond.

	100. 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, Please see in the document, under answer 94 above.
D i s p u t e s e t t l e m e n t w i t h p l a y e r s	101. What qualifies as a complaint or dispute?	A complaint is any written expression of dissatisfaction submitted by a registered player regarding Luckland'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. Besides, the above applies to all LuckLand players, regardless of whether they interact online or in person.
	102. 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 and Bonuses are monitored for abuse. for assistance the Player may then submit an official complaint using the Operator's Complaint Submission Form. The form is available either as a downloadable form that can be completed and emailed or uploaded, and/or as an online form that can be completed and submitted through the website or player account.

	103. Which communication channels are available?	The Operator offers customer support through email and/or live chat. The Operator also makes an official Complaint Submission Form available to players. Where applicable, the form may be submitted online, uploaded through the player account or complaints page, or sent by email. 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.
	104. What information must players provide?	The Complaint Submission Form 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.

	105. What internal department handles complaints?	The first internal Department involved is the Player Support Team, External dispute resolution body and Compliance Manager . The Team grants fast accessibility, as Players must be able to lodge complaints easily and free of charge, grant fairness as Complaints will be reviewed impartially, and outcomes based on evidence, ensure Timeliness, as complaints will be acknowledged and resolved within reasonable timeframes and Transparency, since Players will be informed of progress and reasons for decisions. The Complaint is handled by 3 different Department in several steps: Step 1: Acknowledgement - Complaints will be acknowledged within 2 business days. Step 2: Investigation - The complaint will be reviewed by the Player Support Team. - Technical, financial, and operational records may be checked. - If complex, the player will be advised of expected resolution timelines. Step 3: Response - A written outcome will be provided within 20 working days of receipt. - The outcome will include: - Findings of the investigation. - Actions taken to resolve the issue. - Escalation information if dissatisfied. The Complaint can the go throyiugh Escalation, if unresolved, complaints may be referred internally or to an external dispute resolution body. The Policy provides a user friendly lodging a Complaint to a dedicated email, 6. Escalation Procedure If a player is not satisfied with the resolution: 1. The complaint may be referred to LuckLand’s Compliance Manager. 2. If unresolved internally, the player may contact the Dispute Resolution Service designated by LuckLand’s regulator or seek remedies under the Consumer Guarantees Act. 7. Record Keeping - All complaints will be documented and retained for at least 3 years.
--	--	---

	- Records include complaint details, investigation notes, and resolution outcomes. - Data will be used to identify recurring issues and improve services. 8. Review & Continuous Improvement - This policy will be reviewed annually to ensure compliance with the CGA and gambling regulatory standards. - Feedback from players and regulators will be incorporated into future revisions. However, depending on the specific topic of the complaint, there may be various internal stakeholders with the specific hard skills to manage it. For the sake of completeness, Players may first contact the “Player Support” by any means in chat or email but then filing the explained Form; Complaints are recorded, investigated, and resolved internally. Escalations follow structured internal procedures and identified independent ADR processes are applied when necessary. Particularly, complaints are handled by the 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 prioritized and handled with appropriate involvement of trained Responsible Gaming or Compliance personnel.
--	---

	106. What are the timelines for acknowledgement, investigation, response, and escalation?	Responsible gaming complaints are treated as priority matters. Within two (2) business 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. Luckland 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. Luckland 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.
	107. How are complaint decisions documented?	Luckland 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.

	108. 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 prioritized 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.
	109. Are unresolved complaints escalated to a CGA-approved contracted ADR provider?	YES

D i g i t a l r e c o r d s o f p l a y e r i n f o r m a t i o n	110. What specific player records are maintained?	The Company maintains complete records of: a. Player registration and KYC documentation. b. All gaming and financial transactions. c. Communications related to gaming activities and complaints. These records are retained for at least five (5) years after the last transaction, in line with Curaçao AML/ CFT and gaming laws. After this period, data will be securely deleted or anonymized unless required for ongoing investigations or legal obligations. Unless a longer period is required for ongoing investigations, regulatory inquiries, litigation, fraud prevention, or to meet statutory obligations, the following minimum retention periods apply: Category Details Retention Period Player Identification and KYC Documentation KYC files, identity verification data, due diligence records and supporting documents related to player onboarding and monitoring. At least five (5) years following the player's last transaction or the closure of the player's account. Gaming and Transaction Records All records relating to wagers, bets, game results, account balances, deposits, withdrawals, session logs, gameplay history and system generated gaming data. Five (5) years. Financial, accounting and Tax Records Financial statements, accounting ledgers, transaction records, payment processor statements and statutory tax-related documents. Five (5) years or any longer period mandated by
---	---	---

		applicable financial or tax laws. Player Communications and Complaints Records Records of customer support interactions, internal complaint logs, dispute correspondence and related supporting documentation. Five (5) years. Security, System and Access Logs System access logs, authentication logs, incident logs and security monitoring records. At least one (1) year, unless otherwise required for operational continuity, forensics or regulatory investigation. Where logs from part of gaming system audits, they shall be retained for five (5) years. Responsible Gaming and Player Protection Records Records relating to self exclusion, Responsible Gaming interventions, affordability assessments Five (5) years and monitoring of player behavior. Vendor and Third-Party Processing Records Contracts, due diligence reports and data processing agreements For the duration of the relationship and for five (5) years thereafter.
	111. Are identity details, registration data, verification records, account status, exclusion status, limits, communications, risk indicators, complaints, responsible gaming interactions, and account changes retained?	YES

	112. Are records complete, accurate, searchable, and exportable?	YES
	113. How long are records retained?	Lukland operates under the National Ordinance on Games of Chance (LOK) in Curaçao, licensed online gaming operators are legally required to retain player data, including account details, wagering history, and financial transactions, for a minimum of 3 years. However, because many operators are also bound by international anti-money laundering (AML) laws and the European General Data Protection Regulation (GDPR), like us, could happen that Player data are stored for up to 5 to 7 years following the closure of your account to ensure compliance with financial and global legal obligations. Besides, Luckland is committed to maintaining the confidentiality, integrity, and availability of information assets. The Company's objectives are to: a. Protect player and company data from unauthorized access or disclosure b. Ensure resilience of gaming platforms, systems, and services c. Comply with all applicable laws and regulatory requirements, including the NODP, GDPR (where applicable), the National Ordinance on Games of Chance, and CGA license conditions. d. Maintain stakeholder trust through robust cybersecurity and data privacy practices.
	114. Who can access or amend the records?	Only those assigned 'access rights' strictly necessary for the purpose and time of the data usage and the Player upon request.
	115. Are audit trails maintained?	YES

D i g i t a l r e c o r d s o f g a m i n g t r a n s a c t i o n s	116. Are all bets, stakes, wagers, game rounds, odds, outcomes, wins, losses, cancellations, refunds, jackpots, bonuses used in gameplay, and game session details recorded?	YES
	117. Do records identify the player, date, time, game, transaction ID, amount, currency, result, and balance impact?	YES
	118. Can records be reconstructed in case of dispute or regulatory inspection?	YES
	119. Are game provider records reconciled with platform records?	YES

D i g i t a l r e c o r d s o f f i n a n c i a l t r a n s a c t i o n	120. Are deposits, withdrawals, reversals, chargebacks, payment failures, fees, currency conversions, crypto transactions, bonus credits, manual adjustments, and refunds recorded?	YES
	121. Do records include date, time, amount, currency, payment method, payment provider, transaction reference, player account, status, and approval history?	YES
	122. Are financial records reconciled with payment service provider data and player wallet balances?	YES
	123. How are unusual transactions flagged?	YES

s		
A v a i l a b i l i t y o f r e c o r d s t o t h e C G A	124. Are the required records continuously accessible?	YES
	125. Can the CGA obtain records without delay when requested?	YES
	126. Are records stored in a format that is readable, complete, and exportable?	YES
	127. Who is responsible for responding to CGA requests?	The Managing Director has the primary access to the CGA portal, through which the CGA logs requests for information and documents
	128. Are access logs and audit trails available?	YES
	129. Are backup records also available?	YES

	130. What procedures apply if the primary system is unavailable? 131.	Recovery Time Objective (RTO) and Recovery Point Objective (RPO) Lukland shall define and maintain appropriate recovery objectives based on system criticality: a. Recovery Time Objective (RTO): The maximum acceptable time to restore critical systems following a disruption shall be defined and aligned with business and regulatory needs. For core gaming and player account systems, the target RTO shall be within a commercially reasonable timeframe (e.g., with 24 hours or less, subject to system classification). b. Recovery Point Objective (RPO): The maximum acceptable data loss in the event of an incident shall be defined and minimized for critical systems. For player and transaction data, the target RPO shall not exceed one business day and shall reflect the frequency of backups performed. RTO and RPO targets shall be reviewed periodically and tested as part of the disaster recovery and restoration exercises. 6.8 Encryption and Data Security also in non primary system All player personal data, financial information and gaming records shall be encrypted. Encryption keys shall be managed securely with restricted access and regular rotation. Applications and systems are subject to secure coding standards, vulnerability scanning and periodic penetration testing.
--	---	--

S e r v e r a n d d a t a c e n t r e r e q u i r e m e n t	132. 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?	Luckland Group B.V. ensures that all critical digital records, including players’ personal data, gaming transaction data and financial records are stored on a Tier-IV certified data center located in Curaçao, in compliance with the Curaçao NOGC and the Curaçao Gaming Authority License Conditions. To reduce the risk of data loss and ensure continuity of operations: a. Backups shall be stored in a secure and segregated environment separate from production systems. b. At least one copy of critical backups shall be maintained in an offsite or geographically separate location. c. Redundancy mechanisms shall be implemented to protect against single points of failure. Where cloud-based backup services are used, meet the Company’s security and regulatory requirements and be subject to appropriate contractual safeguards. These records shall always be accessible to the Curaçao Gaming Authority upon request for audit, inspection or investigation purposes. In addition, the Company maintains technical and organizational measures to protect stored data against unauthorized access, accidental loss or damage.
--	--	--

	133. What evidence confirms the certification and registration?	Luckland, can find their official certifications in Curaçao directly on their website or through official accreditation bodies. The certifications—including their Uptime Institute Tier-IV, ISO 27001:2022, and ANSI/TIA-942 Rated-4credentials—can be verified here: Official Facilities & Overview, view the specific certifications listed on them. Corporate Details & Accreditations, read more about their facility standards on the software About Page. Global Certifier Database, view the official ANSI/TIA-942 certificate via the EPI Certification Register. Besides upon request they provide Luckland with what we are looking to verify a specific certification for a compliance audit, or need technical documentation to support your IT infrastructure planning
	134. Which records are stored there?	A variety of mission-critical and highly sensitive records for clients across the Pan-Caribbean and Latin America. Instead of a single type of data, it houses diverse workloads requiring high security and continuous availability. The facility is primarily used to store and process: Financial Records, Banking, FinTech, and RegTech transaction data that require maximum fault tolerance and regulatory compliance. Government & Institutional Data, Sensitive civic records and central administrative databases. Online Gaming & iGaming Data, Player logs, transactional databases, and backend systems for Curacao-licensed online gaming operators. Business Continuity Backups, off-site, continuously replicated data for enterprise disaster recovery and remote working environments. Because the facility sits safely outside the traditional hurricane belt and is both ISO 27001 and SOC 2 certified, it is designed to keep enterprise production and archival workloads continuously online without unplanned downtime
	135. Are mirrored, backup, or replicated records also maintained?	YES

	136. Who manages the server?	Access to player personal data and gaming records is strictly limited to authorized personnel whose duties require such access. Access to systems and data shall be granted on a “need-to-know” and “least privilege” basis. Only the Company approved devices that meet defined security standards may be used to access systems containing player data, gaming records, or financial information. The use of personal or unmanaged devices for such access is prohibited unless expressly authorized and subject to equivalent security Information.Luckland also uses: Security Management System (ISMS): A systematic approach to managing sensitive company information including people, processes, and IT systems.controls.
--	-------------------------------------	---

	137. What security, access control, monitoring, and business continuity measures apply?	Business continuity in Lukland is the capability of a studio or platform to maintain operations and deliver live-service experiences during disruptions. It focuses on preventing downtime, protecting player data, and recovering essential functions rapidly after crises like cyberattacks, server failures, or natural disasters. A robust business continuity framework for gaming studios typically relies on several core pillars to protect revenue and player retention: 1. Core Focus Areas Player Retention & Trust: Live games lose revenue and player base by the minute during outages. Continuity plans prioritize the availability of login servers, matchmaking, and microtransaction storefronts. Disaster Recovery (DR): Dedicated protocols for restoring game servers, databases, and digital assets from secure, geographically redundant backups in the event of hardware failure or ransomware. Live Operations (LiveOps) Continuity: Ensuring the development team can hotfix bugs, deploy seasonal content, and manage the community safely, even if they cannot access physical studio offices. 2. The Four Pillars of BCP Assessment, identifying hazards, analyzing risks, and determining how specific outages (e.g., cloud provider downtime) will financially and operationally impact. Preparedness, creating and updating playbooks, runbooks, and contingencies to prepare staff for critical incidents before they happen. Response, executing the established plans to isolate the problem, communicate with the player base, and mitigate immediate damages. Recovery, restoring operations to predefined capacity, analyzing the root cause, and improving systems to prevent future disruptions
--	--	--