

OPERATIONAL MANUAL

Goodwin N.V. - B2C Remote Games of Chance

Curacao indefinite-term online gaming license

Item	Details
Company	Goodwin N.V.
Registration number	151353
License type	Indefinite-term online gaming license for remote games of chance
License number	OGL/2024/758/0228
Approved domains and applications	immerion.com immerion3.com iwildcasino.com iwildcasino11.org lussurio.com snatchcasino.com
Version	1.0
Effective date	23 June 2026
Approved by	  Morganite Corporate Services B.V. Managing Director Vladyslav Nebrat, UBO

This Operational Manual describes the operating model, controls, procedures, records and reporting arrangements used by Goodwin N.V. to conduct B2C remote games of chance in or from Curacao in a safe, responsible, transparent, verifiable and reliable manner.

1. Document Control

Control	Requirement
Owner	Vladislav Nebrat, UBO
Review frequency	At least annually and whenever there is a material regulatory, operational, technical, supplier, domain, product, payment, AML/CFT/CPF, responsible gaming or license-condition change.
CGA inspection readiness	This Manual and its appendices must be made available to the CGA within five working days of the CGA request.
Change reporting	Changes to this Manual are included in the change reports submitted to the CGA not later than 15 June and 15 January, or earlier where the change requires prior CGA approval.

2. Regulatory Basis and Scope

This Manual is prepared for Goodwin N.V. as the Curacao operator and contractual counterparty to players. It is intended to satisfy Article 5.9 of the National Ordinance on Games of Chance (NOGC/LOK) and the CGA license conditions for an indefinite-term online gaming license.

- National Ordinance on Games of Chance, including Articles 1.2-1.5, 2.1-2.6 and Chapter 5 on Remote Games of Chance.
- License conditions for an indefinite-term online gaming license published by the Curacao Gaming Authority and effective as of 17 December 2025.
- National Ordinance on Identification in Service Provision (NOIS), National Ordinance on the Notification of Unusual Transactions (NORUT), Sanctions National Ordinance (SNO), applicable AML/CFT/CPF rules and CGA instructions.
- Internal policies listed in Appendix 1, including AML/CFT, Responsible Gaming, Complaints, Information Security, Bonus and Cryptocurrency Risk Management policies.

The Manual applies to all B2C brands, websites, domains, subdomains, mobile applications, products, employees, contractors, suppliers and outsourced functions used by Goodwin N.V. for licensed remote games of chance.

3. Company and Licensed Offering

Topic	Description
Licensed operator	Goodwin N.V., a company incorporated under the laws of Curacao. The player-facing gaming agreement is entered into by Goodwin N.V.
Trade names / brands	Immerion, Lussurio, IWILD Casino, Snatchcasino
Approved domains / subdomains	immerion.com immerion3.com iwildcasino.com iwildcasino11.org

	lussurio.com snatchcasino.com
Products	B2C remote games of chance, including online casino, slots, live casino, sportsbook, poker, instant/crash-style games, tournaments, promotions, bonus mechanics and other games approved or permitted under the license.
Target markets and languages	All territories except restricted geos; English is maintained as a regulatory and contractual language. Other target-market languages are supported where required.
Restricted jurisdictions	As defined in the Terms and Conditions, AML/CFT Policy, sanctions screening rules and geo-blocking configuration, and updated when laws, sanctions, provider rules or risk appetite change.

4. Governance and Minimum Roles

Goodwin N.V. maintains the role coverage necessary to comply with the NOGC, CGA license conditions and the Company's operating risk profile. One person may cover more than one operational function where permitted by law, license conditions and internal conflict-of-interest rules. Key Person roles that are legally or operationally incompatible must not be combined.

Role	Minimum responsibility	Assigned person
Board / Managing Director	Overall accountability for licensed operations, resources, player-fund safeguarding, supplier approval, policy approval and CGA engagement.	Norine Clifton
NOGC Compliance Officer	Monitors compliance with the NOGC, license conditions, CGA checklist items, Manual maintenance, change reporting and CGA requests.	Rassul Abumuslim
NOIS/NORUT Compliance Officer / MLRO	Owens AML/CFT/CPF framework, KYC, sanctions, transaction monitoring, goAML reporting, internal suspicious activity handling and AML training.	Rassul Abumuslim
Information Security Owner	Owens information security, incident response, access controls, supplier security oversight, infrastructure inventory and disaster recovery coordination.	Baxiyk Tuzelgaliyev
Responsible Gaming Lead	Owens vulnerable-player controls, limits, self-exclusion, responsible	Baxiyk Tuzelgaliyev

	gaming disclosures, RG monitoring and escalation.	
Complaints Officer	Owns complaint intake, acknowledgement, investigation, decisions, records, reporting and ADR implementation once the CGA-approved approach is confirmed.	Baxiyik Tuzelgaliyev
Payments and Player Funds Owner	Owns player account controls, payment method rules, reconciliation, segregation/ring-fencing, withdrawal operations and crypto payment controls.	Rassul Dursunov

5. Games, Software and Outcome-Determining Elements

The Company offers remote games of chance through approved domains and applications. The offering is maintained in a game inventory that identifies each game or game category, supplier, platform, certification status, game rules, RTP/odds information, supported currencies, payment possibilities, minimum and maximum bet ranges, payout mechanics, software and outcome-determining elements. The minimum inventory format is included in Appendix 3.

- Third-party games and gaming content are supplied only by approved or disclosed suppliers and are certified by laboratories approved by the CGA or by the relevant supplier certification framework.
- Examples of supplier-side laboratories and certification evidence include certificates made available by providers such as Altacore N.V., Dama N.V. and other game suppliers used by the Company.
- Outcome-determining elements, RNG components, live-casino integrations, sportsbook feeds, poker logic, bonus engines and game wallets are documented in supplier technical documentation available for inspection.
- The Company does not offer games whose outcome depends on prohibited events, disasters, exploitation or offensive content, and does not offer credit to players.

Control	Implementation
Game inventory	Maintained continuously; provided to CGA upon request.
Certification evidence	Collected from providers/labs before release and refreshed upon material changes or certificate expiry.
Game rules and RTP/odds	Displayed or made accessible to players through the player interface and/or game provider interface.
New game approval	Subject to internal review, supplier approval checks, certification checks and CGA approval/reporting where required.

Payment possibilities and bet/payout ranges	Maintained per brand/domain and game vertical, including supported fiat/virtual currencies, minimum and maximum bet ranges, payout mechanics and withdrawal constraints.
Outcome-determining elements	Documented per vertical and provider, including RNG, live dealer stream/control systems, sportsbook odds/feed provider, poker engine, instant-game logic and bonus-engine rules.
Periodic quality monitoring	Performed according to Appendix 4 and evidenced through certificates, release checks, vulnerability/security reviews, reconciliation checks, incident trend review and backup/restore testing.

6. Player Interface and Public Disclosures

Goodwin N.V. maintains correct and up-to-date public information on its gaming interface and on approved websites/applications. The following information must be accessible in English and, where required, in the relevant target-market language:

- registered company name, trade name, Chamber of Commerce number, geographic address and contact/customer support details;
- statement that the CGA is the licensing authority and supervisor, together with the required CGA digital seal;
- Terms and Conditions, Privacy/Data Protection notice, Responsible Gaming Policy, AML-relevant player obligations, Bonus Policy, Complaints Policy and other required policies;
- prohibition of participation by minors, self-excluded players, banned players and other vulnerable persons;
- game rules, odds/RTP where available, method of determining winnings, costs of participation, payout timing and payout currency;
- complaints and disputes procedure, including access to ADR at the Company's expense through the interim independent dispute-resolution process described in this Manual, subject to replacement or adjustment if the CGA prescribes or confirms a specific ADR provider or process;
- available limit-setting, cooling-off, self-exclusion and marketing opt-out tools.

7. Player Registration, KYC and Acceptance

A player must register for a player account and log in before participating in remote games of chance. Registration and acceptance are governed by the Terms and Conditions, AML/CFT Policy, AML/CFT Manual, Responsible Gaming Policy and Cryptocurrency Risk Management Policy.

Area	Procedure
Minimum age	Players must be at least 18 years old and must have reached the legal gambling age in their jurisdiction.
Registration data	Mandatory registration information is collected before account activation. Anonymous or fictitious accounts are not permitted.

One-account rule	Only one player account per player is permitted. Duplicate account controls include checks using identity details, email, phone, IP, device, address, payment instrument and other risk indicators.
KYC verification	Identity verification may include government-issued photo ID, proof of address, liveness/biometric verification, payment-method ownership checks and additional enhanced due diligence where required.
Sanctions and restricted jurisdictions	Players are screened against applicable sanctions and restricted-territory rules. Sanctioned, prohibited or unsupported jurisdictions are blocked or rejected.
Source of funds/wealth	Requested based on risk, transaction activity, thresholds, AML triggers, crypto activity, unusual behavior or withdrawal/deposit patterns.
Ongoing monitoring	Customer data and transactional behavior are monitored throughout the relationship, including changes in risk profile, location, payment methods, wallet activity and gaming patterns.

8. AML/CFT/CPF, Sanctions and goAML

Goodwin N.V. is registered and operationally prepared for goAML reporting where applicable. The AML/CFT framework is risk-based and follows the Company's AML/CFT Policy and AML/CFT Manual.

- The MLRO / NOIS-NORUT Compliance Officer maintains the AML/CFT/CPF risk assessment, player risk matrix, enhanced due diligence triggers and reporting procedures.
- Staff are trained to identify suspicious activity, sanctions indicators, fraud, mule behavior, high-risk crypto patterns, source-of-funds concerns and unusual transaction patterns.
- Internal suspicious activity reports are escalated to the MLRO. External reporting is made through the prescribed reporting channel, including goAML where required.
- Records of KYC, EDD, transactions, internal and external reports, player communications and monitoring decisions are retained for at least the period required by law and internal policy.

9. Player Accounts, Payments, Crypto and Safeguarding of Player Funds

All payment transactions between the Company and players are carried out through player accounts. The Company does not act as a financial institution, does not provide credit to players and does not offer investment alternatives. Player funds must be protected from operational use and must remain available for withdrawal and prize payments in accordance with the Terms and Conditions and applicable law.

Control	Required implementation
Segregation / ring-fencing	Player funds, including deposits, winnings and other amounts owed to players, are held in a segregated account or equivalent safeguarded arrangement designated for player liabilities only.

	These funds are not used for ordinary operating expenses, supplier payments or corporate treasury purposes.
Liquidity coverage	The Company maintains sufficient liquidity at all times to pay player balances and reasonably expected winnings. Finance monitors player liabilities against safeguarded funds and available liquidity.
Reconciliation	Player balances, payment processor balances, crypto processor balances, bank/merchant accounts and gaming wallet records are reconciled regularly, with exceptions investigated and escalated.
Same-method / same-currency principle	Withdrawals are made to the same method and, under the license conditions, prize money is paid in the same fiat or virtual currency used to play, unless a lawful exception applies.
No exchange service	The Company does not exchange currencies in the player account or otherwise, and does not exchange virtual currencies for fiat currencies. In-game tokens may be used where permitted and documented.
Crypto acceptance	Only permitted cryptocurrencies that meet the Company's risk criteria may be accepted. Privacy coins, NFTs and DeFi tokens are not permitted unless expressly approved under policy and law.
Crypto KYC/wallet controls	Crypto users complete KYC before transacting. Wallet verification, blockchain analytics, sanctions wallet screening and enhanced checks are applied according to risk.
Freezing and suspension	Accounts, wallets or transactions may be frozen or suspended where AML/CFT, fraud, sanctions, chargeback, responsible-gaming or legal concerns arise.

For CGA purposes the conservative position is to document an operational segregation model, daily or regular reconciliation, a liquidity threshold covering player liabilities, management escalation when coverage falls below threshold, and an express prohibition on using player funds for operating expenses.

10. Responsible Gaming and Vulnerable Persons

The Company implements responsible gaming through its Responsible Gaming Policy, Terms and Conditions, player-account tools, customer support processes and risk monitoring. The purpose is to prevent minors, self-excluded players, banned players and other vulnerable persons from gambling, and to allow players to limit or discontinue gambling where harm indicators arise.

Control	Implementation
General information	Responsible gaming information, addiction-risk information and help resources are made available on the website/app and in player communications.

Limits	Players can set responsible gaming limits, including deposit/loss/wager/session or other available limits as implemented in the player account.
Cooling-off and time-outs	Temporary breaks are made available according to the platform configuration and Responsible Gaming Policy.
Self-exclusion	A player who requests self-exclusion due to problematic gambling is excluded for at least twelve months. During the exclusion period the request is irrevocable.
Marketing suppression	Self-excluded players and players who opt out must not receive marketing material.
Vulnerable-person detection	Customer support, compliance and automated monitoring identify signs of problem gambling, underage activity, third-party account use, loss of control, repeated failed limits, distress statements and other risk indicators.
Internal escalation	Responsible gaming concerns are escalated to the Responsible Gaming Lead and, where appropriate, account limitations, cooling-off, self-exclusion, suspension or closure are applied.

11. Marketing, Affiliates, Bonuses and VIP Activity

Marketing and bonus activity must not encourage excessive gaming, must not be misleading and must not target minors, self-excluded players or other vulnerable persons. The Bonus Policy governs welcome offers, cashback, VIP offers, Fortune mechanics, referral programs, tournaments, free spins, IMR bonus-account mechanics and other promotions.

- All bonus offers are subject to clear terms, including eligibility, wagering requirements, max cashout, time limits, restricted countries, excluded games, withdrawal conditions and anti-abuse rules.
- Players may decline bonuses. Winnings from bonuses are withdrawable only after applicable wagering requirements and verification checks are completed.
- Bonus abuse, multi-accounting, fraudulent activity, self-referrals and manipulation may lead to bonus cancellation, confiscation of bonus-derived winnings and account restrictions where permitted by the Terms and Conditions.
- VIP and affiliate/streamer activities are reviewed for responsible-advertising risk, AML/CFT risk, vulnerable-person risk and misleading-promotion risk.
- Marketing lists are screened against self-exclusion, closed accounts and opt-out records before campaigns are sent.

12. Complaints, Disputes and ADR

The complaint process follows Article 5.3 NOGC and the Goodwin Players Complaint Policy. Players may file complaints free of charge within six months after the relevant incident, bet settlement or event conclusion. Complaints may relate to deposits, withdrawals, bonus terms, account restrictions, game errors, responsible gaming, player balances, KYC, data protection, technical malfunctions, AML concerns, alleged fraudulent games or breach of license conditions.

Step	Procedure
Submission channels	Live chat, complaints@immerion.com, support@immerion.com and other official channels published by the Company.
Eligibility	Only the registered account holder may submit a complaint, unless the Company accepts another legally valid representation.
Required information	Player identity/account, contact details, date, description of the behavior complained of, relevant bet/transaction IDs and supporting documents where available.
Acknowledgement	Written acknowledgement is sent within one week, together with an explanation of the handling process.
Decision period	The Company provides a written final decision within four weeks, or extends once in writing for a further four weeks.
Records	Complaints, investigation records, decisions, player communications and outcomes are retained for at least five years or longer where required.
ADR status	The Company provides players with access to ADR at its own expense through an interim independent dispute-resolution process. Until the CGA prescribes or confirms a specific ADR provider/process, unresolved disputes are escalated to an independent external reviewer or dispute-resolution provider appointed by the Company and independent from the operational decision under dispute. The Company will replace or adjust this arrangement immediately if the CGA issues a mandatory ADR provider, template or procedure. ADR records and outcomes are retained and reported to the CGA as required.

13. Information Security, Infrastructure and Business Continuity

The Company maintains administrative, technical and organizational security controls proportionate to B2C remote gaming operations. The Information Security Policy governs confidentiality, integrity and availability of information assets, vendor security and security incident response.

Area	Control
Infrastructure inventory	The Company maintains an inventory of gaming equipment, application software, databases, interfaces, integrations, suppliers and environments.
Curacao data access	Critical player, gaming-transaction and financial-transaction data remain accessible to the CGA through a server hosted in an authorized Tier-IV certified data center located in Curacao.
Access control	Access is role-based, least-privilege, reviewed periodically and removed upon role change or termination.
Encryption and secure transmission	Player and transaction data are protected using secure transmission and appropriate encryption/security controls.

Monitoring	Systems are monitored for availability, integrity, suspicious access, payment anomalies, fraud indicators and security incidents.
Backups	Backups of customer data, transaction data, compliance data and critical records are made securely and regularly according to internal policy.
Disaster recovery	The Company maintains restoration procedures for technical emergency situations, including escalation, supplier coordination, backup restoration and service recovery.
Incident response	Security, fraud, personal-data, game-integrity and service-availability incidents are assessed, documented, remediated and reported to the CGA within 24 hours where required.

14. Technical Emergency and Restoration Procedure

1. Detect and classify the incident: security breach, software/equipment failure, data compromise, game outage, payment disruption, fraud/crime event or other serious threat to responsible, reliable and verifiable operations.
2. Activate the internal incident team: Information Security Owner, NOGC Compliance Officer, affected operational owner, supplier contact and management representative.
3. Contain the issue: suspend affected functionality, freeze affected accounts or transactions, block suspicious access and preserve logs/evidence.
4. Assess player impact: affected games, bets, balances, personal data, payment transactions, bonus balances, pending withdrawals and communications required.
5. Restore service: use backups, failover, supplier recovery, configuration rollback or controlled release procedures as appropriate.
6. Report: file a CGA incident report within 24 hours where required and update the report as investigation and remediation progress.
7. Post-incident review: identify root cause, corrective actions, player remediation, supplier actions, policy updates and training needs.

15. Suppliers, Critical Services and Outsourcing

The Company uses third-party suppliers for platform services, gaming content, payment processing, KYC/AML, blockchain analytics, hosting, information security, customer support, affiliate/CRM tools and other functions. All supplier relationships are subject to risk-based onboarding, contractual controls and ongoing monitoring.

- Critical Services or Goods are not purchased from unregistered or non-approved suppliers where registration or approval is required by law, license conditions or CGA instruction.
- Prior CGA approval is obtained where required before entering relationships concerning gaming platforms, game/content provision, payment processing or financial transactions.

- Supplier files include ownership/registration information, contracts, scope of services, data-processing/security terms, certification evidence, business continuity contacts and incident-notification obligations.
- Outsourcing does not transfer regulatory responsibility: Goodwin N.V. remains responsible for compliance with applicable laws, license conditions and player obligations.

16. Records, Retention and CGA Access

The Company keeps records so that its rights and obligations, player rights and regulatory compliance can be verified at all times. Records are maintained in a secure, accessible and retrievable form. Appendix 5 describes the minimum storage matrix for player personal data, game transactions, financial transactions, compliance records, supplier records and CGA-accessible critical data hosted through the Curacao Tier-IV data-center arrangement.

Record type	Minimum content
Player records	Registration details, KYC/EDD, verification evidence, risk rating, account status, restrictions, self-exclusion and limits.
Gaming records	Bets, wagers, game participation, game outcomes, prize payments, bonuses, IMR/bonus-account activity and game errors.
Financial records	Deposits, withdrawals, payment method data, payment processor records, crypto wallet screening, reconciliations, chargebacks and player liabilities.
Compliance records	AML reports, sanctions checks, internal suspicious activity reports, goAML submissions where applicable, training records and policy approvals.
Complaints records	Complaints, acknowledgements, investigation notes, final determinations, ADR records and CGA complaint/ADR reports.
Supplier records	Supplier due diligence, approvals/registrations, contracts, certificates, service reviews and incidents.
Retention period	At least five years after account closure, last transaction or the applicable event, unless a longer legal, regulatory or internal retention period applies.

17. CGA Reporting Calendar

Report	Frequency / trigger
Change report / amendment report	Twice per year, not later than 15 June and 15 January, including changes to the Operational Manual and a new version where required.
Incident report	Within 24 hours of the incident or, where investigation is required, from confirmation, except where the license conditions deem the period to start at occurrence.
Player transaction report	As required by CGA template/instructions; includes amount, nature of credit/debit, payment instrument and non-directly identifying payment account identifier per approved domain/application.

Complaints report	As required by CGA template/instructions.
ADR report	As required once the ADR provider/process is confirmed and operational.
Annual financial statements	Submitted to CGA by 30 June of the next calendar year.
Independent expert AML/NOIS/NORUT report	Submitted periodically upon request and according to CGA instructions.
Independent expert system design / responsible gambling report	Submitted periodically upon request and according to CGA instructions.
Other CGA requests	Provided within the deadline stated by CGA or within a reasonable period under the NOGC.

18. Training

The Company provides annual permanent education to persons working in the field of games of chance, adjusted to their role and expected knowledge level. The current training program being implemented covers:

- anti-bribery and crime prevention;
- AML/CFT/CPF, sanctions, suspicious activity escalation and goAML awareness;
- player communications and complaints handling;
- responsible advertising, bonus and affiliate controls;
- responsible gaming, vulnerable persons, limits and self-exclusion;
- information security and incident escalation where relevant to the role.

Training attendance, content, completion dates and assessment results are retained as compliance records.

19. Change Management

The Company applies internal review and approval before making material changes to operations. Prior CGA consent is obtained where required, including changes or additions involving UBOs, qualified-interest holders, directors, Key Persons, domains, suppliers, articles of association or any other matter determined by the CGA.

8. Business owner identifies proposed change and prepares description, rationale, affected systems/domains/suppliers/policies and expected date.
9. Compliance assesses whether prior CGA approval, license amendment, portal update or change report is required.
10. Information Security, AML, Responsible Gaming, Payments and Supplier owners review impact where relevant.
11. Management approves implementation after regulatory requirements are satisfied.
12. Operational Manual, policies, website disclosures, supplier inventory, game inventory and training material are updated where affected.
13. Change is included in the next amendment report or reported earlier if required.

20. Internal Monitoring and Inspection Readiness

The NOGC Compliance Officer maintains a compliance monitoring schedule. The schedule covers license conditions, public disclosures, player registration and KYC, responsible gaming tools, complaints, ADR operation and readiness for CGA-prescribed ADR changes, reporting, supplier files, game certificates, security controls, player-fund safeguarding and training records.

- The Manual and appendices are stored in a controlled repository with version history.
- Evidence files are maintained so the Company can respond to CGA requests within the applicable deadline.
- Findings are tracked to closure and escalated to management where overdue or material.
- The Company cooperates with CGA inspections and provides requested data, records, access and assistance.

Appendix 1 - Source Policies and Documents

Document	Reference
Terms and Conditions	1 December 2025 / uploaded PDF
Bonus Policy	Uploaded PDF
Responsible Gaming Policy	Version 1.0, effective 29 September 2025
Information Security Policy	Version 1.2, effective 29 September 2025
AML/CTF Policy	Goodwin N.V., uploaded PDF
AML/CFT Manual	Approved May 2025, Goodwin N.V., registration number 151353
Players Complaint Policy	Version 1.0, effective 30/31 July 2025
Cryptocurrency Risk Management Policy	Version 1.0, effective 15 April 2025
National Ordinance on Games of Chance	Publicatieblad 2024 No. 157, official translation supplied as LOK.pdf
CGA indefinite-term online gaming license conditions	CGA portal, effective 17 December 2025

Appendix 2 - Training Matrix

Audience	Training topics
Board / management	License conditions; governance; player funds; incidents; AML overview; responsible gaming oversight; CGA reporting
Compliance / MLRO	AML/CFT/CPF; sanctions; goAML; KYC/EDD; reporting; recordkeeping; CGA engagement
Customer support	Player communications; complaints; KYC escalation; responsible gaming; vulnerable persons; account closures
Marketing / VIP / affiliates	Responsible advertising; bonus rules; vulnerable-person targeting prohibition; AML and RG escalation

Payments / fraud	Player funds; withdrawals; crypto risks; chargebacks; fraud; transaction monitoring; account freezing
IT / security	Information security; access control; incident response; backup/restore; supplier security

Appendix 3 - Game, Payment, Software and Outcome Inventory

This inventory is maintained as a live controlled schedule for each approved domain and application. It satisfies the minimum Operational Manual requirement to describe the games offered, payment possibilities, bet amounts, payouts, software and outcome-determining elements. The operational owner updates the schedule before launch of a new game vertical, provider, payment method or material game change, and Compliance reviews whether CGA approval or reporting is required.

Vertical / product	Suppliers / software	Outcome-determining elements	Payment possibilities, bet amounts and payouts
Online casino / slots	Game suppliers include Altacore N.V., Dama N.V. and other approved/disclosed providers.	Provider RNG, certified game math, game rules, RTP, bonus-feature logic and platform wallet integration.	Supported currencies and crypto assets: USDT, USDC, TON, etc. Min/max bet ranges and payout rules are displayed in the game interface or provider rules. Winnings are credited to the player account and paid in accordance with T&C and license conditions.
Live casino	Live casino provider(s): Hollycorn N.V. (Softswiss), SoftGaming	Live dealer process, certified game procedures, studio controls, shoe/wheel/table controls, streaming integration and provider settlement logic.	Bet limits are set by provider table/game rules and displayed to players. Payouts follow game rules and are credited to the player account.
Sportsbook / betting	Sportsbook software/feed provider(s): Hollycorn N.V. (Softswiss), SoftGaming.	Odds feed, event data, bet acceptance rules, settlement rules, risk/trading	Bet limits, markets, payout calculations and settlement timing are displayed through sportsbook rules and T&C.

		controls and void / cancellation rules.	
Poker / peer-to-peer games	Poker engine/provider (s): Hollycorn N.V. (Softswiss), SoftGaming.	Certified shuffle/RNG, table logic, rake/fee logic, tournament rules, collusion/fraud monitoring and settlement engine.	Buy-ins, blinds, rake, fees and payout structures are displayed in the poker interface/tournament rules.
Bonuses, tournaments and IMR mechanics	Bonus engine / CRM / promotion tools: Goodwin N.V.	Eligibility, wagering, max cashout, tournament ranking, free-spin allocation, IMR conversion/use rules and anti-abuse logic.	Bonus values, wagering requirements, time limits, withdrawal conditions and payout limitations are stated in Bonus Policy and promotion-specific terms.

Appendix 4 - Periodic Testing and Quality Monitoring

The following controls are the minimum recurring test methods used for quality monitoring. Evidence is retained in the compliance evidence repository and made available to CGA upon request.

Test / monitoring method	Minimum frequency / trigger	Owner	Evidence retained
Game/provider certification review	Before launch; upon certificate expiry; upon material game/provider change; at least	Supplier Owner / Compliance	Certificates, provider attestations, game inventory, approval checklist.

	annually for active providers.		
Game release and configuration QA	Before release of new games, bonus mechanics, payment methods or material configuration changes.	Product / Platform Owner	UAT checklist, release approval, rollback plan, screenshots or logs.
RTP/game rules/public disclosure check	Before launch and periodically for active game categories.	Product / Compliance	Disclosure checklist, screenshots, provider rules/RTP files.
Payment and wallet reconciliation	Daily or other documented regular cycle proportionate to transaction volume; immediately for material exceptions.	Payments and Player Funds Owner	Reconciliation reports, exception logs, escalation notes.
Player-fund safeguarding coverage review	At least monthly and whenever material payment/withdrawal stress or operational change occurs.	Payments Owner / Management	Coverage report, safeguarded-balance evidence, liquidity review.
Information-security vulnerability review	According to Information Security Policy; after material release; after critical vulnerability; at least annually for independent testing where applicable.	Information Security Owner	Scan reports, pen-test reports, remediation tracker.
Access-rights review	At least quarterly and upon staff/vendor role change.	Information Security Owner	Access review sign-off, joiner/mover/leaver records.
Backup and restore test	At least annually and after material	Information Security Owner	Restore test evidence, RTO/RPO

	infrastructure change.		assessment, issues log.
Responsible-gaming monitoring review	At least monthly and upon serious RG incident.	Responsible Gaming Lead	RG case log, intervention record, limit/self-exclusion records.
Complaints trend review	At least quarterly or when material complaint pattern appears.	Complaints Officer	Complaints register, root-cause analysis, corrective actions.
Incident trend and post-incident review	After each reportable incident and at least quarterly.	NOGC Compliance Officer / InfoSec	Incident report, root-cause analysis, corrective-action tracker.

Appendix 5 - Data Storage, Retention and CGA Access Matrix

This matrix describes how critical player, game and financial data are stored and made accessible. System names, data-center references and evidence links must be kept current in the live evidence file.

Data category	Primary system / location	Access and security controls	Retention	CGA access / evidence
Player registration and personal data	Platform / back-office / KYC system	Role-based access, MFA where available, least privilege, audit logs, encryption / security controls according to Information Security Policy.	At least five years after account closure or last transaction, unless a longer period applies.	Replicated or accessible through Curacao Tier-IV data-center arrangement where required.
KYC, EDD, sanctions and AML records	KYC/AML provider and compliance repository	Restricted compliance access, audit logs, controlled export, secure	At least five years or longer if required by AML/CFT/CPF rules,	Available to CGA/FIU where lawful and required

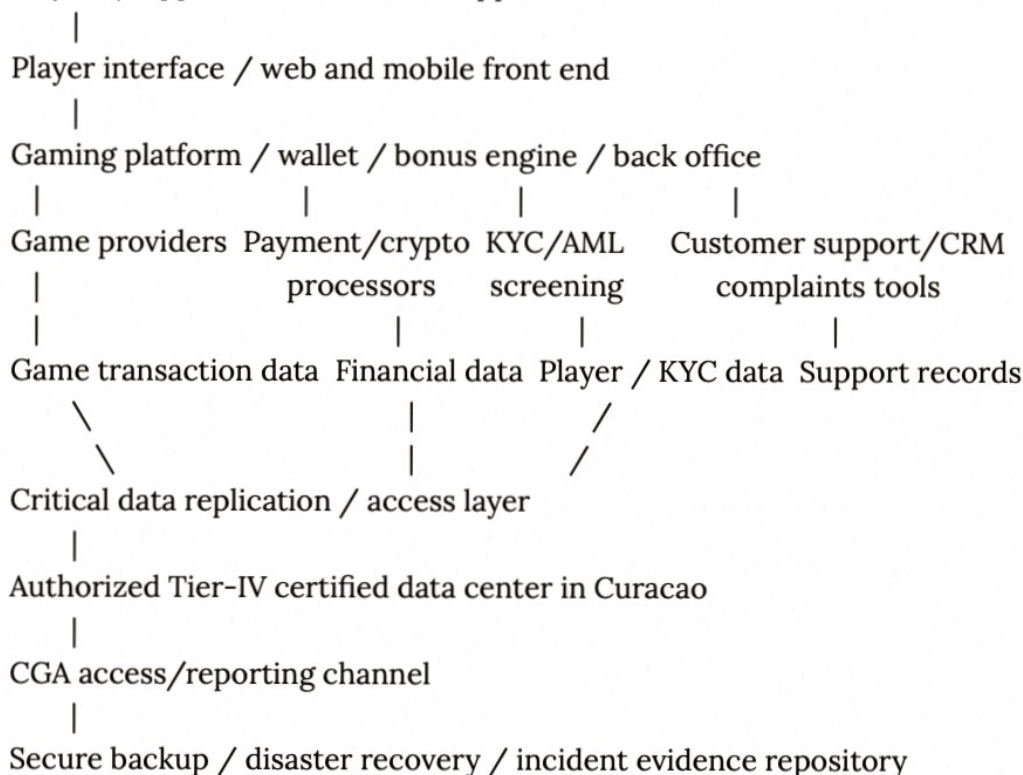
		storage of ID and verification evidence.	investigation hold or regulatory request.	
Game transactions and outcomes	Gaming platform / provider data stores	System logs, integrity controls, supplier access restrictions, audit trails.	At least five years or longer if required for disputes, AML, tax/accounting or CGA request.	Critical data accessible through Curacao Tier-IV data-center server
Financial transactions and player account balances	Wallet / payment / back-office systems	Segregated access by payments/compliance, reconciliation controls, transaction audit trails, exception escalation.	At least five years after account closure/last transaction or longer if required.	Player financial transaction data accessible to CGA through Curacao Tier-IV data-center arrangement
Payment instruments and crypto wallet screening	PSP / crypto processor / blockchain analytics provider	Provider security controls, limited internal access, wallet screening, sanctions checks and EDD triggers.	At least five years or provider/legal retention period if longer.	Available through processor reports and compliance repository
Complaints and ADR records	Support / complaints register	Complaints Officer controlled access, case audit trail, supporting evidence retained.	At least five years or longer if dispute/regulatory hold applies.	Complaint and ADR reports provided to CGA as required

Supplier and certification records	supplier due diligence repository	Controlled access by Compliance/Supplier Owner, version-controlled certificates and agreements.	Term of relationship plus at least five years, or longer if required.	Supplier register, approvals and certifications available for inspection.
Training and compliance monitoring records	HR & compliance repository	Compliance-controlled access, attendance logs, assessment records and sign-offs.	At least five years or longer if required.	Available to CGA upon request.

Appendix 6 - Technical Infrastructure Diagram and Restoration Map

The following high-level diagram is the minimum infrastructure map for Article 5.9. The Company must maintain a live technical diagram with actual system names, hosting locations, supplier names, interfaces, data flows, backup/DR locations and CGA-access mechanisms.

Players / approved domains and apps



Component	Minimum description / evidence required	Restoration / emergency procedure
Approved domains/apps	Current CGA-approved list, DNS/control evidence and public disclosure screenshots.	Redirect/suspend affected interface; notify players if needed; restore from approved deployment pipeline.
Gaming platform and wallet	Platform supplier, version, hosting, wallet/balance logic, access controls and audit logs.	Failover/restore according to RTO/RPO; reconcile balances before reopening affected functionality.
Game providers	Supplier list, certification evidence, game rules/RTP, integration points.	Disable affected provider/game; preserve logs; coordinate provider investigation; report if incident threshold met.
Payment/crypto processors	Processor list, supported currencies/assets, segregation/safeguarding evidence and reconciliation data.	Suspend affected payment method; freeze suspicious transactions; reconcile balances; use alternative approved methods if available.
KYC/AML tools	Provider, screening coverage, sanctions/goAML workflow, EDD records.	Manual review fallback; queue onboarding/withdrawals; escalate high-risk cases to MLRO.
Curacao Tier-IV access server	Data-center authorization/Tier-IV evidence, data categories accessible, synchronization frequency and CGA-access procedure.	Restore synchronization; validate data completeness; notify CGA if access is materially impaired.
Backup/DR repository	Backup schedule, encryption/security, restore test evidence and responsible owner.	Activate restore plan; document root cause and recovery results; perform post-incident review.

Appendix 7 - Player Funds Safeguarding Evidence

This appendix translates the player-fund safeguarding requirement into evidence that can be inspected. The Company must not use player funds for ordinary operating expenses, supplier payments or corporate treasury purposes.

Requirement	Minimum operational control
Segregated account or equivalent safeguarded arrangement	Player deposits, winnings and other amounts owed to players are held in a segregated account or equivalent safeguarded PSP/crypto arrangement designated for player liabilities.
Coverage of player liabilities	Finance monitors player liabilities against safeguarded balances and available liquidity sufficient to pay balances and reasonably expected winnings.
Regular reconciliation	Player balances, PSP balances, crypto wallets, bank/merchant accounts and platform wallet records are reconciled on a documented regular cycle.
Exception escalation	Material reconciliation breaks, liquidity shortfalls, stuck withdrawals or processor issues are escalated to Payments Owner, Compliance and Management.
Withdrawal controls	Withdrawals are processed according to T&C, AML/KYC controls, same-method/same-currency rules and account-freezing rules where justified.