

Novi.B.V. Operational Manual

For Remote Gaming Licence Holder Compliance under Article 5.9(1) LOK

Name	Description
Document Name	Curaçao Operational Manual
Version	1.0
Review Date	01.06.2026

Version	Description	Date	Updated By
1.0	Implementation	20.06.2026	Compliance

1. Purpose and Scope

1.1 Purpose

The purpose of this Operational Manual is to document how Novi BV conducts remote gaming operations under its Curaçao remote gaming licence and how it maintains compliance with the requirements of the Landsverordening op de kansspelen / National Ordinance on Games of Chance ("LOK"), applicable licence conditions, regulatory instructions, internal policies and operational control standards.

This Manual sets out the systems, processes, controls, responsibilities and records used by the Licence Holder to operate its remote gaming business in a controlled, transparent, secure and compliant manner.

2. Corporate and Licence Information

- Company Name: Novi B.V.
- Company license number: 155510
- Registered Office Address: Dr. M.J. Hugenholtzweg 25, Curaçao
- License Type: Curaçao Gaming Authority
- License Number: OGL/2024/1288/0542
- License Granted: 11/09/2024
- Approved Brands: Miki & Kazancasino
- Approved Domains: miki.com/kazancasino.com
- Directors: Virae Management B.V.

3. Platform & Infrastructure Set-up

3.1 Overview

The Licence Holder operates remote casino brands using a third-party Player Account Management system. The platform supports player registration, account management, wallet functionality, KYC status tracking, responsible gaming tools, bonus management, game integration, reporting and operational risk controls.

Novi B.V. retains operational responsibility for the remote gaming activity conducted under its licence, including player onboarding, AML monitoring, responsible gaming oversight, payments, complaint handling, reporting and regulatory compliance.

3.2. Platform Architecture

The platform utilizes a cloud-hosted, service-oriented architecture where independent systems handle distinct operational domains, communicating through controlled interfaces and a central messaging layer. This decoupled design isolates functions—such as player accounts, wallets, payments, game delivery, bonuses, and back-office administration—allowing each to be operated, scaled, and audited independently.

When a player accesses our public brands (**Miki** and **Kazancasino**), their requests pass through a secure public gateway responsible for encryption and routing. Registration and identity requests are directed to authentication services, after which the **Player Account Management (PAM)** system maintains the authoritative record of the player's status and limits.

Financial transactions flow seamlessly from the **Payment System** to the **Wallet**, which connects to external providers and records all ledger entries. Similarly, the **Game Service** coordinates with licensed game suppliers to securely settle bets and results back to the player's wallet.

Throughout this journey, systems operate in parallel as the **Player Engagement System** handles user bonus offers, while an independent **Rules Engine** drives real-time automated decisions. Both systems communicate asynchronously with the rest of the platform via the central messaging layer to protect performance. To ensure robust security, back-office administration is completely isolated from the public internet, providing authorized staff with separate, secure modules for fraud detection, AML monitoring, CRM management, and customer support.

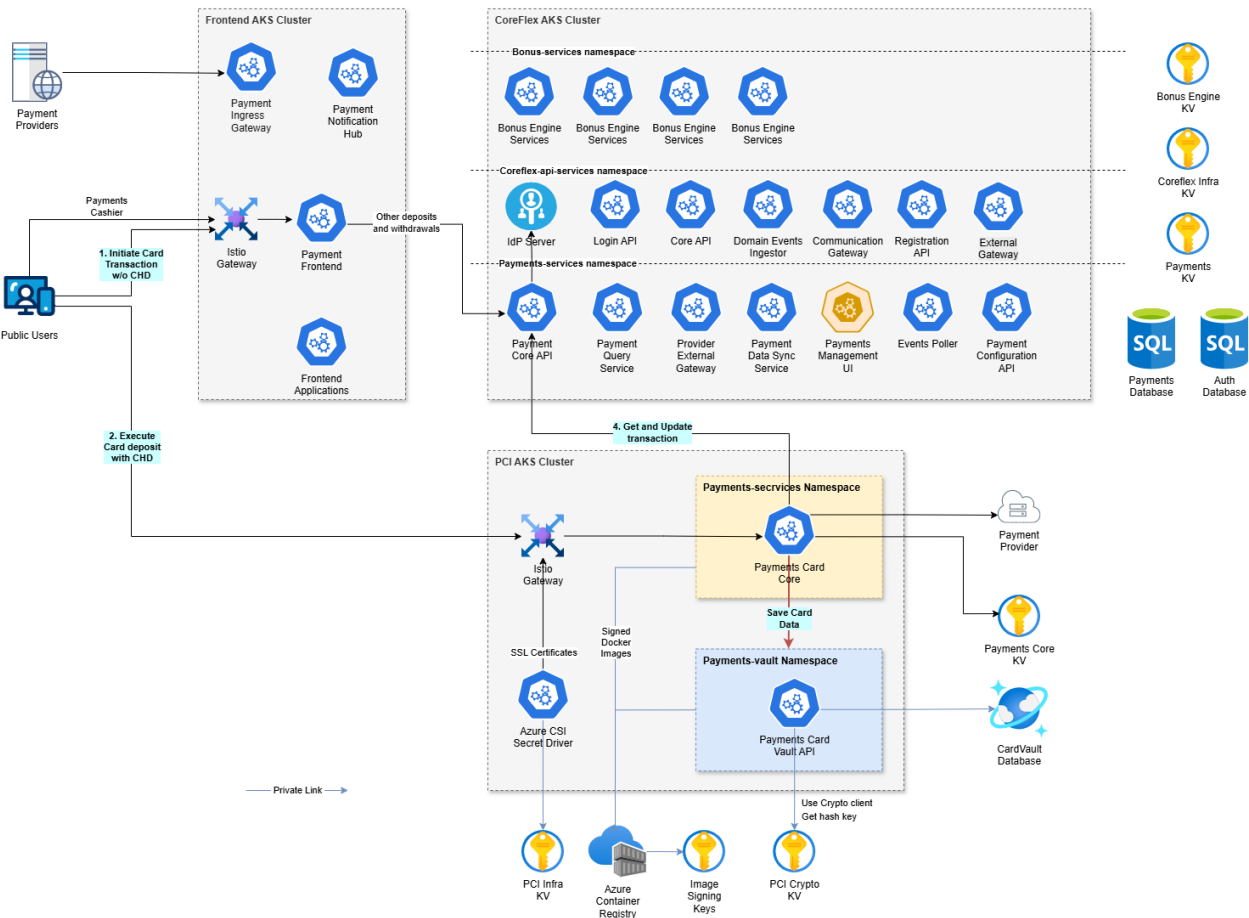
3.3 System Architecture

The remote gaming operation relies on the following principal systems. Each performs a defined role and generates records that allow the Licence Holder to demonstrate control and compliance.

System	Function	Evidence retained to demonstrate control / compliance
Player Account Management (PAM)	Authoritative record of each player, account status, KYC/verification status and applied limits	Player account records, verification history, account-change audit trail
Registration & Authentication	Player onboarding, login and secure access control	Registration records, authentication audit logs, access records
Wallet & Payment Services Platform	Deposits, withdrawals, balances and transaction processing via external payment providers	Transaction history, provider transaction logs, payment audit trail
Game Service / Game Integration	Connects to licensed game suppliers, manages game sessions, and records bets, results and settlement	Game transaction records, game session/audit history, supplier launch and configuration records
Bonus & Promotions Engine	Bonus issuance, wagering tracking and expiry	Bonus award, wagering and adjustment records
Rules / Decision Engine	Real-time decisions supporting the other systems	Decision request and outcome records

Back-office System	Operational administration, player review, reporting and account controls	Back-office action and audit logs
--------------------	---	-----------------------------------

The systems are hosted in a cloud environment as described in Section 4, and access to each is controlled and logged. Records generated by these systems are retained in line with Section 9 and are retrievable for audit or regulatory request.



4. Domains, Hosting and Technical Environment

The technical environment is hosted on Microsoft Azure using a managed Kubernetes platform, leveraging the tier-one provider's robust physical security, resilience, and compliance certifications. To ensure operational stability, separate and isolated environments are

maintained for development, testing, and production, guaranteeing all changes are thoroughly validated before reaching live players.

Technical and administrative access is strictly restricted based on the principle of least privilege, with authentication consolidated through a corporate Identity Provider. Furthermore, application secrets and credentials are completely abstracted from code or configuration files, housed securely within a managed key service, and rotated periodically.

Continuous logging and application-performance monitoring ensure high availability, with all telemetry data strictly processed within the EU and validated by independent external monitoring.

Infrastructure and software integrity are maintained via automated patching during defined weekly maintenance windows, alongside controlled deployment pipelines that require formal approval prior to production releases.

Finally, the ecosystem is heavily protected by advanced network controls, mandatory data encryption in transit, and complete segregation between public player-facing domains and sensitive administrative environments.

5. AML/Risk & Fraud Framework

5.1 Player Registration, Onboarding and Account Controls

Novi B.V. collects personal details, third-party declaration, T&Cs acceptance and confirmation that the person is over 18 at registration.

During registration and post-registration checks, Novi B.V. applies account acceptance controls to prevent underage gambling.

Players must be registered before real-money play, and under-18, sanctioned individuals, individuals from non-reputable/restricted jurisdictions, players who fail to provide identification information, or those who provide fake documents.

Identity verification confirms:

- Full name
- Nationality
- Date of Birth
- Residential Address

Age verification is completed through approved government-issued identification before first withdrawal and upon reaching applicable regulatory thresholds. Where it is discovered that a minor has registered an account, the account is closed immediately, deposits are refunded, winnings are forfeited and a clear explanation is provided.

5.2. KYC, CDD and Enhanced Due Diligence

KYC and CDD checks are completed to verify the identity, age, address, nationality and payment ownership of customers. Verification is required at the latest once the customer reaches the applicable cumulative transaction threshold, currently set at Naf 4000, unless verification has already been completed at registration or first payout stage using approved electronic identification technology. Where required documentation is not provided within the required timeframe, the account may be restricted, terminated or escalated in accordance with the AML policy.

The name registered must match the government-issued ID. Verification documents can be requested at any time, and withdrawals may be held pending satisfactory verification.

Enhanced Due Diligence is applied where the customer, jurisdiction, transaction, payment method, product use or screening result indicates a higher risk of money laundering, terrorist financing, proliferation financing or fraud. EDD may include additional identity verification, source of funds, source of wealth, payment ownership checks, adverse media review, third-party database checks and MLRO approval.

5.3. PEP and Sanctions Screening

Customers are screened against PEP and sanctions data as part of the AML control framework. Potential PEP matches are escalated for enhanced review, and potential sanctions matches are restricted and escalated to the MLRO. True positive sanction matches are handed in accordance with the AML Policy and applicable legal obligations.

5.4. Ongoing Monitoring

Customer risk profiles are monitored on an ongoing basis. The frequency of review is determined by the customer's assigned risk rating, with higher risk customers subject to more frequent review and enhanced oversight. Automated and/or manual monitoring is used to identify linked accounts, unusual account activity, high-risk country indicators, transaction alerts and other suspicious patterns.

Risk Rating	Review Frequency
Low Risk	Every three years
Medium Risk	Every two years
High Risk	Every year or upon transaction alerts
High Risk - Enhanced	Monthly or upon transaction alerts

5.5. Customer Risk Assessment

Customers are risk assessed using a risk-based methodology that considers customer profile, jurisdiction, product use, payment method and transaction behaviour. Risk ratings are used to determine the level of due diligence, monitoring and escalation required.

5.6. Reporting Unusual Transactions

Where unusual or suspicious activity is identified, the matter is escalated to the MLRO within 24 hours. The MLRO will assess the matter, document the investigation and determine whether a report to the FIU is required. Employees, officers and directors are prohibited from informing the customer or any third party that a report has been or may be submitted.

5.7. AML Training

AML training is provided to relevant employees to ensure they understand their obligations, including customer identification, verification, suspicious activity indicators, internal escalation, STR reporting, tipping off restrictions and recordkeeping.

6 . Responsible Gaming and Player Protection

Novi B.V. maintains a Responsible Gambling Policy to ensure that gambling offered under our license is conducted responsibly, safely, and transparently, in accordance with the requirements of the Curaçao Gaming Authority (CGA).

6.1. Responsible Gambling Information and Accessibility

A dedicated Responsible Gambling Section is available on the operator's websites. This section provides clear information on responsible gambling, direct access to tools including deposit limits, cooling-off, and self-exclusion, contact information for responsible gambling support, and links to local and international problem gambling support services. The section is available in English and other languages, and is linked from the homepage, Terms & Conditions, and site

footer. The website footer also includes a prohibition statement against underage gambling, the operator's registered details and license number, the CGA's digital seal, and links to recognised gambling support organisations.

6.2. Player Self-Assessment and Account History

Players are provided with access to at least six months of wagering and transaction history through their account. Extended records are available upon request within ten working days. Self-assessment questionnaires are made available to help players review their gambling behaviour and consider whether responsible gambling tools should be applied.

6.3. Behaviour Monitoring and Intervention

Novi B.V. actively monitors player behavior to identify indicators of problematic gambling, including sudden increases in deposits or wagering, frequent failed transactions, cancelled withdrawals, extended gambling sessions, frequent Responsible Gambling Tools usage, or agitated and frequent communications with customer support. Intervention procedures include providing information about responsible gambling tools, applying mandatory limits or restrictions, temporarily suspending accounts where necessary, and permanently excluding players in cases of severe or persistent risk. All interventions are recorded in the Player Account Management (PAM) system. Responsible gambling measures will never be used to delay or prevent legitimate withdrawals.

6.4. Deposit Limits

Players may set daily, weekly or monthly deposit limits. Once the relevant limit is reached, further deposits are blocked until the limit period resets. Requests to reduce deposit limits take effect immediately, while requests to increase limits are subject to a 24-hour cooling-off period. Deposit limits apply across all brands and domains operated under the licence.

6.5. Cooling-Off

Players may apply a cooling-off period for 24 hours, 7 days, 1 month or 3 months. During the cooling-off period, gambling functionality is disabled while withdrawal access remains available. The account is automatically reactivated once the selected period expires.

6.6. Self-Exclusion

Players may self-exclude for 1 year, 3 years, 5 years, 10 years or lifetime. Self-exclusion can be completed through account settings or by contacting the operator. Once applied, the account is closed, login access is disabled and marketing communications are stopped. Reactivation after

the exclusion period requires a written request from the player and review in accordance with internal procedures.

6.7. Operator-Initiated Exclusion

Novi B.V. may impose an operator-initiated exclusion where there are clear signs of gambling-related harm or other material player protection risks. The reason for the exclusion, supporting evidence, decision-maker and player communication are documented and retained.

6.8. Responsible Marketing

All marketing, promotional and affiliate activity must be conducted responsibly and in accordance with applicable CGA requirements. Marketing must not target minors or vulnerable persons, present gambling as a financial solution or investment, misrepresent games of chance as games of skill, or encourage excessive gambling. Promotions must clearly state applicable terms and conditions and display responsible gambling messaging.

6.9. Training

Customer-facing staff receive mandatory responsible gambling training. Training covers identification of problem gambling indicators, procedures for interacting with at-risk players, escalation routes and guidance on directing players to responsible gambling tools and external support organisations.

7. Payment and Wallet Processes

Novi BV offers a number of deposit and withdrawal methods to the player - which includes cards, wallets and bank transfers.

A player can make a deposit or a withdrawal from their player account by logging in and carrying out the relevant transaction. It is not possible for the player to receive funds on their player account in form of cash or transfer from another player. Deposits from corporate accounts are also not accepted - in such instances, the deposit will be refunded. As additional controls, to ensure legitimacy of the funds, all card deposits require a 3ds confirmation and only 1 wallet per wallet type is permitted to be registered on a player account at any given time. In cases where a player requests to register an additional wallet, the player is requested to submit proof of ownership to ensure that the wallet belongs to the player.

Novi B.V. also has Risk and Fraud procedures in place to mitigate payment fraud. This includes asking for Proof of Payment ownership where necessary, enforcing closed loop on certain

payment methods (ex. wallets) and ensuring that the player deposit is wagered at least 1x before the funds can be withdrawn.

The operator also has controls in place to ensure that the same payment method is not registered on multiple accounts.

Novi B.V. does not directly process any payments - the business fully utilises third party PSPs. As part of onboarding any PSPs, the company carries out its due diligence on the PSP provider to ensure that the partner is credible and operates as per licence requirements. When a player is making a deposit or a withdrawal, the player goes to the Novi B.V. operator cashier, selects the relevant method and is redirected to the 3rd party PSP pages, embedded on the operator site, to complete the transaction. The PSP then processes the transaction on their end.

8. Games, Software and Outcome Systems

Novi B.V. offers remote games of chance through approved third-party game suppliers and/or casino aggregation partners. The games, game software, random number generation systems, live casino systems, game outcome systems and related technical components are provided and maintained by third-party suppliers rather than developed directly by Novi B.V.

Novi B.V. remains responsible for ensuring that all games made available under its Curaçao remote gaming licence are supplied by appropriately approved, licensed or contracted third-party providers and, where required, certified by a testing laboratory approved or recognised by the Curaçao Gaming Authority

Novi B.V. does not alter, manipulate or interfere with game outcomes. Game outcomes are generated by the relevant game supplier's certified systems, including RNG, live dealer, jackpot, crash game or other outcome systems, as applicable. Novi B.V. relies on supplier certifications, game approvals, contractual controls, supplier disclosures and operational monitoring to ensure that games are fair, secure, auditable and operated in accordance with applicable requirements.

Novi B.V. maintains oversight through supplier due diligence, contractual controls, game certification records, CGA portal supplier disclosures, game registers, launch approvals, incident escalation processes and access to game transaction evidence.

9. Data Storage, Records and Retention

The Novi B.V. maintains and retains operational, customer, financial, compliance, AML/CFT, responsible gambling, transaction, audit, and regulatory records as required by applicable laws, licence conditions, regulatory requirements, and internal policies.

Records may include, without limitation:

- Customer account and registration records;
- Customer identification and verification (KYC) documentation;
- Transaction and payment records;
- Gaming activity and wagering records;
- Responsible gambling records;
- AML/CFT monitoring and investigation records;
- Customer complaints and communications;
- Internal compliance and audit records;
- Regulatory correspondence and reporting records; and
- Corporate and operational records.

As a general principle, customer identification, transaction and AML/CFT records are retained for a minimum of five (5) years following account closure, termination of the business relationship, or completion of the relevant transaction, unless a longer retention period is required by law, regulation, legal proceedings, regulatory investigations, or legitimate business needs.

Records are stored electronically in secure cloud-based and/or on-premises infrastructure. and/or approved service providers. Appropriate technical and organisational measures are implemented to protect records against unauthorised access, alteration, disclosure, loss, or destruction. Backup copies are maintained and tested periodically in accordance with the Novi B.V.'s business continuity and disaster recovery procedures.

Access to records is restricted on a need-to-know basis and is controlled through role-based permissions, authentication controls, and activity logging. Access rights are reviewed periodically by authorised personnel.

Novi B.V. aims to retrieve active records within 48 hours and archived records within 5 Business Days, subject to the nature and scope of the request.

Upon expiry of the applicable retention period, records are securely deleted, anonymised, or otherwise disposed of in accordance with Novi B.V.'s Data Retention and Disposal procedures. Where applicable, disposal activities are documented and retained for audit purposes.

10. Cyber Security and Disaster Recovery

Security is integrated into every layer of our system through continuous, automated testing and a battle-tested incident response protocol. If an incident occurs, it is instantly classified by severity (P1 to P4), driving a structured response from a dedicated team through containment, eradication, and controlled recovery. This entire ecosystem is validated annually to ensure peak operational readiness.

11. Complaint Handling and ADR Procedures

Novi B.V. maintains a complaints handling process to ensure that player complaints are received, recorded, investigated and resolved in a fair, transparent and timely manner.

Players are encouraged to contact Customer Support in the first instance through live chat or email, as many service issues may be resolved at first contact. Where a player wishes to raise a formal complaint, the complaint must be submitted from the player's registered email address to with "**Complaint**" included in the subject line.

Formal complaints must be submitted within six months of the incident giving rise to the complaint.

11.1 Complaint Submission Requirements

To support efficient investigation, players are requested to provide the following information when submitting a formal complaint:

- Full name
- Username
- Residential address
- Country of Residence
- Clear description of the issue
- Relevant dates and times
- Supporting evidence

11.2 Responsible Gaming Complaints

Responsible gambling-related complaints are handled with priority. These may include complaints involving deposit limits, cooling-off, self-exclusion, account reopening, RG interactions, marketing suppression, underage gambling, or any concern that the operator failed to identify or respond to potential gambling-related harm.

Where a complaint relates to responsible gambling, Customer Support must escalate the matter to the Responsible Gambling Officer or Compliance Officer for review. The complaint file must include the player's RG status, limit history, exclusion history, relevant communications, account activity and any previous interventions.

Responsible gambling complaints must not be treated only as service complaints. They must also be reviewed to determine whether there has been any failure of player protection controls.

11.3 Escalation to ADR

If a player is not satisfied with Novi B.V.'s final response, the player may escalate the complaint to the appointed independent Alternative Dispute Resolution provider.

The appointed ADR provider is CADRE, which provides a free-of-charge alternative dispute resolution service.

Players may submit a complaint to CADRE using the ADR provider's online claim process. Players may be required to show that they have completed the Licence Holder's internal complaints process before submitting a case to ADR.

Novi B.V. records ADR referrals and outcomes in the Complaints Register or ADR Register.

11.4 Regulatory Authority

The Curaçao Gaming Authority does not resolve individual player disputes, but players may contact the CGA regarding regulatory concerns or potential regulatory breaches.

Where a complaint indicates a potential regulatory breach, compliance failure, system failure, responsible gambling failure, payment control issue, AML concern or other material incident, the Compliance Officer assesses whether internal escalation, remediation or regulatory notification is required.