

OPERATIONS MANUAL

hype.bet

Operated by BlackSands B.V.

Remote Games of Chance • Curaçao

Curaçao Gaming Authority (CGA)

Gaming Licence No. **OGL/2024/985/0430**

Version 1.0

Effective Date: June 29th 2026

Prepared and maintained pursuant to Article 5.9 of the National Ordinance on Games of Chance (Landsverordening op de Kansspelen), P.B. 2024 No. 157

STRICTLY CONFIDENTIAL

Commercial-in-Confidence. For the Curaçao Gaming Authority and authorised personnel only.

Table of Contents

1. Document Control.....	4
1.1 Document Identification	4
1.2 Version History	4
1.3 Distribution	4
1.4 Approval.....	5
1.5 Regulatory Cross-Reference	5
2. Purpose and Scope	6
2.1 Purpose	6
2.2 Scope.....	6
2.3 Legal and Regulatory Framework	6
2.4 Definitions	6
3. Company Overview.....	8
3.1 Corporate Structure	8
3.2 Licensed Activities	8
3.3 Domains and Applications	8
4. Governance and Responsibilities	10
4.1 Board of Directors.....	10
4.2 Key Persons	10
4.3 Compliance Function.....	10
4.4 Substance Requirements (Art. 5.12)	10
5. Player Registration and Account Management.....	12
5.1 Account Opening	12
5.2 Account Activation	12
5.3 Ongoing Monitoring	12
6. Player Data Management	13
6.1 Data Collection	13
6.2 Data Storage.....	13
6.3 Data Retention.....	13
6.4 Confidentiality and Breach Handling	13
7. Gaming Platform Description	14
7.1 Platform Overview	14
7.2 Player Interface and Visual Elements	14
7.3 Game Integrity and Testing	14
8. Responsible Gaming Program	15
8.1 Policy Statement.....	15
8.2 Player Protection Measures	15
8.3 Identification of Problem Gambling	15
8.4 Staff Training	15
8.5 Marketing and Advertising Standards (Art. 5.6)	16
9. Excluded and Prohibited Players.....	17
9.1 Restricted Persons	17
9.2 Technical Controls.....	17
10. AML / CFT Program	18
10.1 Risk-Based Approach	18
10.2 Customer Due Diligence.....	18
10.3 Monitoring.....	18

10.4 Reporting	18
11. Payments and Financial Controls	19
11.1 Deposits	19
11.2 Withdrawals	19
11.3 Segregation of Funds and Player-Fund Protection	19
11.4 Bonuses and Wagering	19
12. Complaints and Dispute Resolution	20
12.1 Internal Complaints Procedure	20
12.2 Escalation and Timelines	20
12.3 Alternative Dispute Resolution	20
12.4 Governing Law and Jurisdiction	20
13. Technical Infrastructure	21
13.1 Infrastructure Diagram	21
13.2 Hosting Environment	21
13.3 Security Controls	21
14. Business Continuity and Disaster Recovery	22
14.1 Incident Classification	22
14.2 Disaster Recovery	22
14.3 Recovery Objectives	22
15. Record Keeping	23
16. Incident and Regulatory Reporting	24
17. Training Program	25
18. Review and Updates	26
Appendices	27
Appendix I - Domain Register	27
Completion Checklist (remove before filing)	27

1. Document Control

This document is the **Operations Manual** required to be maintained at all times by the holder of a licence for Remote Games of Chance under Article 5.9(1) of the National Ordinance on Games of Chance (the “**LOK**”). It records the manner and degree of compliance by BlackSands B.V. (the “**Operator**”, operating the brand “**hype.bet**”) with the LOK and the rules and restrictions attached to its Gaming Licence.

In accordance with Article 5.9(3), this Manual shall be made available for inspection by the Curaçao Gaming Authority (the “**CGA**”) within five (5) working days of a first request. Changes are notified to the CGA through amendment reports submitted twice per year, no later than 15 June and 15 January, together with the updated Manual (Article 5.10(4)).

1.1 Document Identification

Field	Detail
Document title	hype.bet - Operations Manual
Operator (licensee)	BlackSands B.V.
Brand / trading name	hype.bet
Company registration No.	162520 (Curaçao Chamber of Commerce)
Gaming Licence No.	OGL/2024/985/0430
Regulator	Curaçao Gaming Authority (CGA)
Registered office	Abraham de Veerstraat 1, Willemstad, Curaçao
Document owner	Compliance Officer / MLRO
Approved by	Managing Director
Classification	Strictly Confidential - Commercial-in-Confidence
Version	1.0
Effective date	June 29 th 2026
Last review date	Not applicable (initial issue)
Next review date	Within twelve (12) months of the effective date

1.2 Version History

Version	Date	Summary of changes	Author / Approver
1.0	June 29 th 2026	Initial issue of the Operations Manual.	Compliance / Managing Director
			 Morganite Corporate Services B.V. Managing Director

1.3 Distribution

This Manual is distributed on a need-to-know basis to:

- The Curaçao Gaming Authority (on request, and as an attachment to amendment reports);
- The Board of Directors of BlackSands B.V.;
- The Compliance Officer / Money Laundering Reporting Officer (MLRO);
- Heads of Operations, Payments, Customer Support, and IT / Information Security;

- Other personnel and contractors to the extent required to perform their roles.

1.4 Regulatory Cross-Reference

The table below maps the minimum content requirements of Article 5.9(1) of the LOK, and other principal obligations, to the sections of this Manual. It is intended to assist the CGA in verifying completeness.

LOK provision	Requirement	Manual section
Art. 5.9(1)(a)	Description of games offered, payment options, bet amounts, payouts, software and outcome-determining elements	§3.2, §7.1, §11
Art. 5.9(1)(b)	Periodically used test methods for quality monitoring	§7.3
Art. 5.9(1)(c)	Manner of storing players' personal data	§6
Art. 5.9(1)(d)	Visual elements shown to players	§7.2
Art. 5.9(1)(e)	Technical measures preventing admission of banned persons	§9.2
Art. 5.9(1)(f)	Technical infrastructure diagram and restoration capability	§13.1, §14
Art. 5.9(1)(g)	Implementation of responsible gaming (Arts. 2.2(3), 5.4, 5.6)	§8
Art. 5.9(1)(h)	Current text of general terms and conditions	Appendix K (§3.3)
Art. 5.9(1)(i)	Dispute settlement with players (Art. 5.3)	§12
Art. 5.9(1)(j)	Critical digital records on a Tier-IV data centre in Curaçao	§6.2, §13.2, §15
Art. 5.4	Vulnerable persons policy and self-exclusion	§8, §9
Art. 5.6	Marketing and advertising conduct	§8.5
Art. 5.10	Reporting (incidents within 24h; amendments 15 Jun / 15 Jan)	§16
Art. 5.11	Record-keeping; annual financial statements by 30 June	§15
Art. 5.12	Substance requirements (key persons, premises)	§4.4
Art. 5.9(4)	Annual permanent education of staff	§17
NORUT / NOIS / Sanctions / goAML	Anti-money laundering and counter-terrorist financing	§10

2. Purpose and Scope

2.1 Purpose

This Manual describes the operational, technical, governance, compliance, responsible gaming, anti-money laundering and player-protection procedures implemented by the Operator in connection with the offering of Remote Games of Chance under its Gaming Licence, in accordance with the requirements of the CGA and applicable Curaçao law.

2.2 Scope

This Manual applies to:

- All Remote Games of Chance offered by the Operator under Gaming Licence No. OGL/2024/985/0430;
- All domains, sub-domains and applications operated under the Licence (see §3.3 and Appendix I);
- All directors, officers, employees, agents and contractors of the Operator involved in the gaming operation; and
- All critical service providers and suppliers, to the extent of their interaction with the licensed activity.

2.3 Legal and Regulatory Framework

The Operator conducts its business in accordance with, among others:

- **National Ordinance on Games of Chance** (Landsverordening op de Kansspelen), P.B. 2024 No. 157 (the LOK), and ministerial regulations and national decrees issued under it;
- **National Ordinance on the Reporting of Unusual Transactions** (NORUT), P.B. 2017 No. 99;
- **National Ordinance on Identification during the Provision of Services** (NOIS), P.B. 2017 No. 92;
- **Sanctions National Ordinance** (P.B. 2014 No. 55) and the **Kingdom Sanctions Act** (P.B. 2016 No. 54);
- **National Decree on the goAML Reporting Portal** (P.B. 2020 No. 157); and
- Applicable data-protection requirements and the confidentiality obligations of Article 14.1 of the LOK.

2.4 Definitions

Capitalised terms used in this Manual have the meaning given in Article 1.1 of the LOK, including in particular:

Term	Meaning (per LOK Art. 1.1, summarised)
CGA	Curaçao Gaming Authority (Stichting Gaming Control Board), the independent regulator.
Remote Game of Chance	A game of chance provided remotely by electronic communication and played without physical contact with the provider.
Vulnerable Person	A person under 18; or who lacks sufficient control over gambling behaviour; or who is excluded from play; or who is bankrupt / has lost disposal of property.
Ultimate Beneficial Owner (UBO)	A natural person ultimately owning or controlling the entity by holding more than 10% of shares, voting rights or ownership interests.

Term	Meaning (per LOK Art. 1.1, summarised)
Qualified Interest	A direct or indirect interest of at least 10% of share capital or voting rights, or similar control.
Key Person	A natural person with direct or indirect control of, or significant influence on, the licensee's management, assets or operational policy.
Critical Services / Goods	Gaming-related services or goods indispensable to determining the outcome of a game, or whose deficiency may significantly affect the licensee's compliance.
Gross Gaming Revenue (GGR)	Value of bet amounts received less prizes made available in the same period (Art. 5.12(5)).

Operational terms additionally used in this Manual: **KYC** (Know Your Customer), **CDD / SDD / EDD** (Customer / Simplified / Enhanced Due Diligence), **MLRO** (Money Laundering Reporting Officer), **RG** (Responsible Gaming), **RNG** (Random Number Generator), **RTP** (Return to Player), **ADR** (Alternative Dispute Resolution), **RTO / RPO** (Recovery Time / Point Objective).

3. Company Overview

3.1 Corporate Structure

Item	Detail
Legal name	BlackSands B.V. (besloten vennootschap, Curaçao)
Company registration No.	162520
Registered office	Abraham de Veerstraat 1, Willemstad, Curaçao
Shareholders	Worldwide Tech Solutions Ltd – 37,88%, Paradiso Foundation Fundacja Rodzinna – 18,94%, Kukito Foundation Fundacja Rodzinna – 18,94%, Avenue H. Capital LLC – 5,15%, Yolo ME-FZ-LLC – 19,08%
Ultimate Beneficial Owners (>10%)	Jamie Nikanpour – Germany, Łukasz Marek Sobieraj – Poland, Karol Adam Sobieraj – Poland, Travis Beswick - Australia
Directors	Morganite Corporate Services B.V. – Norine Clifton
Key Persons	Morganite Corporate Services B.V. – Norine Clifton, Łukasz Marek Sobieraj, Sylwia Czarnik – Frużyńska, Artem Kuznetsov
Organisational chart	See Appendix A

The identity, existence and involvement of all UBOs, holders of a Qualified Interest, and persons who make or influence policy decisions have been ascertained and are kept current; any change is reported to the CGA in accordance with the Licence conditions and the applicable fees of Article 5.18.

3.2 Licensed Activities

The Operator offers the following Remote Games of Chance, all of which are operated under the Gaming Licence:

- **Online casino - slots:** a library of 15,000+ titles from 100+ studios, including Evolution, NetEnt, Play'n GO, Red Tiger and Pragmatic Play;
- **Live dealer casino:** hosted table products streamed from licensed studios;
- **Table games:** roulette, blackjack and casino poker variants;
- **Hype Originals:** in-house instant / “crash”-style games (e.g. dice, mines, limbo) operated on a provably-fair basis;
- **Casual, lottery-style and crash games;**
- **Virtual sports;**
- **Sportsbook:** powered by BETBY, covering 28 sports plus racing and esports markets (CS2, Dota 2, League of Legends, Valorant), pre-match and in-play;
- **Social features:** multiplayer / streaming rooms, a vault facility.

Prohibited offerings (LOK Art. 1.4)

The Operator does **not** offer games whose outcome depends on a disaster, crisis, or the exploitation/abuse of humans or animals (Art. 1.4(a)); does **not** extend or intermediate credit to players (Art. 1.4(c)); and does **not** allow underage persons or other Vulnerable Persons to play (Art. 1.4(d)-(e)).

3.3 Domains and Applications

The primary domain is **www.hype.bet**. All domains, mirror domains, sub-domains and applications operated under the Licence are listed in the Domain Register (Appendix I). The Operator currently provides a responsive mobile-web experience and **no** dedicated native mobile application. Each registered domain or software application on which games are offered is notified to the CGA, for which the fee under Article 5.18(5) (EUR 250 per domain / application) applies.

The current general terms and conditions applied to players are maintained as Appendix K, satisfying Article 5.9(1)(h).

4. Governance and Responsibilities

4.1 Board of Directors

The Board of Directors holds ultimate responsibility for the lawful and responsible operation of the licensed business, including:

- Strategic oversight and approval of the operating model;
- Ensuring continuing compliance with the LOK and Licence conditions;
- Approval of key policies (responsible gaming, AML/CFT, data protection, complaints, business continuity);
- Enterprise risk management and the maintenance of adequate liquid assets to pay out reasonably expected prizes (Art. 2.2(2)(g)); and
- Oversight of the Compliance function and CGA relationship.

4.2 Key Persons

“Key Persons” (Art. 1.1(p)) are the natural persons who control or significantly influence the Operator's management, assets or operational policy. The Operator maintains an up-to-date register of Key Persons, their roles, reporting lines and decision-making authority. No Key Person is a Vulnerable Person (Art. 2.2(2)(j)), and positions that are incompatible by nature are not held by the same person (Art. 5.12(3)).

Function	Holder	Principal authority
Managing Director	Morganite Corporate Services B.V. – Norine Clifton	Overall management; CGA primary contact
Compliance Officer / MLRO	Łukasz Marek Sobieraj	Compliance, AML/CFT, RG oversight, reporting
Head of Operations	Łukasz Marek Sobieraj	Day-to-day gaming operations
Head of Payments / Finance	Sylvia Czarnik-Frużyńska	Payments, segregation, financial controls
Head of IT / Information Security	Artem Kuznetsov	Platform, infrastructure, security

4.3 Compliance Function

The Compliance Officer / MLRO operates with sufficient independence and authority and is responsible for:

- Regulatory compliance with the LOK and Licence conditions;
- AML/CFT oversight, including acting as MLRO and filing reports through the goAML portal;
- Responsible gaming monitoring and the handling of self-exclusion and intervention;
- Incident and amendment reporting to the CGA (§16); and
- Maintaining this Manual and the underlying policies and records.

4.4 Substance Requirements (Art. 5.12)

Article 2.1(4) requires the Operator to be managed by at least one natural person resident in Curaçao (or a qualifying local entity so managed). Article 5.12 further requires, on a phased basis, that the Operator employ Key Persons appearing in the Curaçao Population Register - at least one in the first four years following entry into force of the LOK, and at least three from the fifth year - in addition to maintaining business premises in Curaçao equipped for the licensed activity.

Substance requirement	Status / arrangement
Curaçao-resident managing director (Art. 2.1(4))	Morganite Corporate Services B.V. – Norine Clifton
Key Person(s) in Curaçao Population Register (Art. 5.12(1)(a)-(b))	[1 in first 4 years; 3 from year 5]
Business premises in Curaçao (Art. 5.12(1)(c))	Abraham de Veerstraat 1, Willemstad, Curaçao
Exemption under Art. 5.12(4) (new / small operator, GGR < ANG 20m)	[state whether the exemption is claimed and the basis]

5. Player Registration and Account Management

5.1 Account Opening

A natural person may hold only one player account. The registration and onboarding process includes:

1. **Registration:** collection of identifying and contact data, and acceptance of the terms and conditions and privacy notice;
2. **Age verification:** confirmation that the player is at least 18 years of age, since persons under 18 are Vulnerable Persons (Art. 1.1(h)(i)) who must be prevented from playing (Art. 1.4(d));
3. **Identity verification (KYC):** verification of identity using reliable, independent documentation and/or electronic verification;
4. **Jurisdiction / geolocation:** confirmation that the player is not located in a Restricted Jurisdiction (see §9.1);
5. **Sanctions and PEP screening:** screening against applicable sanctions lists and politically-exposed-person databases;
6. **Self-exclusion check:** screening against the Operator's exclusion register (§9).

Identification and verification are performed in accordance with the NOIS, and in any case before, or upon, a transaction or related transactions reaching the threshold of ANG 4,000 (Art. 15.4 amending the NOIS), and earlier where the risk profile requires.

5.2 Account Activation

Accounts are activated for deposit and play only after the applicable KYC requirements have been satisfied. Withdrawals are subject to completed verification (§11.2). The Operator applies duplicate-account detection and will close or merge duplicate or fraudulent accounts.

5.3 Ongoing Monitoring

The Operator conducts periodic and event-driven reviews covering:

- Currency and validity of identity documentation;
- Customer risk ratings and re-assessment on trigger events;
- Transaction patterns and deposit/withdrawal behaviour; and
- Geographic and device-related risk indicators.

Persons who qualify as Key Persons of the Operator are prohibited from playing its games (Art. 1.3(b)), and no credit is provided to any player (Art. 1.4(c)).

6. Player Data Management

This section satisfies Article 5.9(1)(c) (manner of storing players' personal data) and supports Article 5.9(1)(j).

6.1 Data Collection

The Operator collects only data necessary for the operation and for legal and regulatory compliance, including:

- Personal identification data (name, date of birth, nationality, identification document details);
- Contact information (email, telephone, address);
- Payment information (crypto wallet addresses, fiat/on-ramp references);
- Device, session and geolocation information; and
- Gaming and transaction activity.

6.2 Data Storage

Player data is stored using:

- Encryption in transit (TLS 1.2 or higher) and at rest;
- Role-based access controls and the principle of least privilege;
- Secure, monitored backup systems; and
- Critical player, gaming-transaction and financial-transaction records held on a server of a **Tier-IV certified data centre registered in Curaçao**, kept available to the CGA at all times (Art. 5.9(1)(j)).

6.3 Data Retention

Records are retained for the periods prescribed by the LOK, AML legislation and applicable data-protection law. As a minimum, player identity (KYC) records, account records and transaction records are retained for the duration of the business relationship and for at least ten (10) years following its termination. Complaint records, responsible-gaming records and other records required to demonstrate regulatory compliance are retained for the same minimum period. At the end of the applicable retention period, personal data is securely deleted or irreversibly anonymised.

6.4 Confidentiality and Breach Handling

All personnel are bound by confidentiality consistent with Article 14.1 of the LOK. Any breach that may have compromised players' personal information is treated as a reportable incident and notified to the CGA within 24 hours (Art. 5.10(5)(a) and (6); see §16).

7. Gaming Platform Description

This section satisfies Article 5.9(1)(a) (games, payments, bet amounts, payouts, software, outcome-determining elements), (b) (test methods) and (d) (visual elements).

7.1 Platform Overview

The Operator runs an in-house platform integrating the following components:

Component	Description
Casino aggregation / RGS	Remote game servers of integrated studios (Evolution, NetEnt, Play'n GO, Red Tiger, Pragmatic Play and others) delivering slots, live dealer and table games.
Sportsbook	BETBY sportsbook platform: 28 sports, racing and esports; pre-match and in-play.
Wallet & payments engine	Crypto and fiat wallet, deposits/withdrawals, blockchain node integrations.
Player account & RG engine	Registration, KYC status, responsible-gaming limits and self-exclusion.

Outcome-determining elements: casino game outcomes are determined by certified RNGs operated by the relevant licensed studios; sportsbook outcomes are determined by real-world event results settled by the sportsbook provider; Return-to-player (RTP) information is published per game. Bet amounts and payout rules per product are recorded in the Game and Limit Configuration Register maintained jointly by the Compliance and IT / Information Security functions and summarised in Appendix L.

7.2 Player Interface and Visual Elements

Representative screenshots and descriptions of the following player-facing elements are maintained in Appendix B and include:

- Registration and login pages;
- Deposit and withdrawal pages (crypto and fiat);
- Responsible-gaming tools (limits, time-out, self-exclusion);
- The complaint submission form; and
- Game lobby, in-game and bet-slip interfaces.

7.3 Game Integrity and Testing

Game integrity is safeguarded by:

- Certified RNGs and approved game providers;
- Provably-fair verification for Hype Originals;
- Publication of RTP and game rules; and
- Periodically used test methods for quality monitoring (Art. 5.9(1)(b)), described in the Operator's Game Testing and Quality Assurance Procedure.

8. Responsible Gaming Program

This section implements the responsible-gaming requirements of Articles 2.2(3), 5.4 and 5.6 and satisfies Article 5.9(1)(g).

8.1 Policy Statement

The Operator is committed to providing a safe, secure and fair gaming environment, to ensuring games are fair and clear to players, to preventing Vulnerable Persons from playing, and to enabling players to limit or discontinue play where it threatens to become an addiction (Art. 2.2(3)).

8.2 Player Protection Measures

The following tools are made available to players:

- Deposit limits (daily / weekly / monthly);
- Loss limits;
- Wager / stake limits;
- Session-time limits and reality-check reminders;
- Cooling-off periods / time-outs; and
- **Self-exclusion:** on a player's written request, exclusion for a period of at least twelve (12) months, which is irrevocable during the exclusion period (Art. 5.4(2)).

8.3 Identification of Problem Gambling

Indicators monitored, including by automated behavioural analytics, include:

- Escalating deposits or rapid deposit frequency;
- Repeated requests to increase limits;
- Chasing losses and escalating stake sizes;
- Play during unusual hours or for unusually long sessions; and
- Distress signals raised through customer support.

Where indicators are detected, the Operator follows a documented intervention workflow that may include messaging, limit prompts, temporary restriction, referral to support resources, and, where appropriate, exclusion. General information about gambling addiction is made available to players (Art. 5.4(1)(a)).

8.4 Staff Training

Customer-facing and relevant operational staff receive annual training on responsible gaming, recognition of problem gambling, mental well-being, player interaction and intervention procedures (see §17).

8.5 Marketing and Advertising Standards (Art. 5.6)

Marketing, advertising and bonusing are conducted so that they:

- Do not encourage excessive gaming;
- Are not misleading; and
- Do not target Vulnerable Persons.

Bonus and promotional terms (including wagering requirements and any forfeiture conditions) are presented clearly and fairly; all communications carry 18+ and responsible-gaming messaging; and

affiliates and marketing partners are contractually bound to the same standards and are monitored for compliance.

9. Excluded and Prohibited Players

This section satisfies Article 5.9(1)(e) and supports Article 5.4(1)(d).

9.1 Restricted Persons

The Operator prevents access by:

- Persons under 18 years of age;
- Self-excluded players (during any active exclusion);
- Persons located in a Restricted Jurisdiction. The Operator does not offer its services in, and applies technical controls (including geolocation and IP-based blocking) to prevent access from, the United States, France, Germany, the Netherlands, Australia and Curaçao itself, together with any jurisdiction subject to applicable financial sanctions or designated by the FATF as high-risk. This list is reviewed periodically and updated as required;
- Key Persons of the Operator (Art. 1.3(b)); and
- Persons subject to applicable sanctions.

9.2 Technical Controls

Admission of barred persons is prevented through technical measures including:

- Identity verification at registration and before withdrawal;
- IP / geolocation checks and device fingerprinting;
- An exclusion database that blocks re-registration by self-excluded players;
- Automated sanctions / PEP screening; and
- Duplicate-account and fraud detection.

10. AML / CFT Program

The Operator maintains an anti-money-laundering and counter-terrorist-financing program consistent with the NORUT, the NOIS, sanctions legislation and the goAML reporting framework. The MLRO is responsible for the program.

10.1 Risk-Based Approach

The Operator maintains a documented AML/CFT risk assessment addressing customer, product, channel, payment (including virtual-asset) and geographic risk, and applies controls proportionate to assessed risk.

10.2 Customer Due Diligence

CDD measures include:

- Identification and verification of the customer (and, where relevant, beneficial owner);
- Verification at or before the ANG 4,000 transaction threshold (Art. 15.4) and earlier on a risk basis;
- Source-of-funds and, where warranted, source-of-wealth review;
- Enhanced Due Diligence (EDD) for higher-risk customers, PEPs and unusual activity; and
- **Virtual-asset controls:** wallet screening and on-chain analytics to assess the provenance of crypto deposits and the destination of withdrawals.

10.3 Monitoring

Ongoing monitoring covers unusual transactions, structuring, fraud indicators, sanctions exposure and high-risk crypto flows, using automated transaction monitoring and blockchain analytics.

10.4 Reporting

Unusual transactions are reported to the Financial Intelligence Unit through the goAML portal in accordance with the NORUT, within the prescribed timeframes. The Operator applies a strict no-tipping-off rule, maintains AML records for the statutory period, and screens against, and reports as required under, the Sanctions National Ordinance and the Kingdom Sanctions Act.

11. Payments and Financial Controls

This section supports Article 5.9(1)(a) and Articles 5.7 and 5.8(g).

11.1 Deposits

The Operator accepts thirteen cryptocurrencies - BTC, ETH, LTC, USDT, USDC, DOGE, SOL, TRX, BNB, TON, XRP, ADA and BCH - across native integrations on Ethereum, TON, Solana, Tron and Binance Smart Chain. The minimum fiat deposit is USD 20 (crypto minimums may be lower). No credit is extended to players, and the Operator does not act as an intermediary in providing credit (Art. 1.4(c)).

11.2 Withdrawals

Withdrawals are subject to:

- Completed identity verification (KYC) of the account holder;
- Fraud and AML review, including source/destination wallet screening;
- Withdrawal limits of USD 10,000 per day and USD 50,000 per month (subject to crypto-value fluctuation); and
- Payout to verified instruments consistent with the deposit source where required.

11.3 Segregation of Funds and Player-Fund Protection

Player funds are held separately from operational funds. The Operator maintains adequate liquid assets to pay out reasonably expected winnings (Art. 2.2(2)(g)) and participates in the guarantee fund for Remote Games of Chance once established and required (Art. 5.7), against payment of the applicable premium, to guarantee payout of player prizes.

11.4 Bonuses and Wagering

Bonus mechanics (welcome offers, challenges, the daily wheel, VIP rewards, vault and tipping) operate under clear, fair and non-misleading terms consistent with Art. 5.6, with wagering requirements and any forfeiture conditions disclosed before opt-in.

12. Complaints and Dispute Resolution

This section satisfies Article 5.9(1)(i) and implements Articles 5.3 and 5.5.

12.1 Internal Complaints Procedure

A player may file a complaint, free of charge, within six (6) months of an incident relating to play (Art. 5.3(1)). Complaints may be submitted by email, through the website complaint form, or via 24/7 live chat, and may be made in English, Dutch or Papiamentu (Art. 5.3(3)(c)). Complaints are logged using the Operator's complaint template, which records the complainant's name and address, the date, and a description of the matter.

12.2 Escalation and Timelines

The Operator handles complaints as follows:

1. **Acknowledgement:** within one (1) week of receipt, with a written acknowledgement and an explanation of how the complaint will be handled (Art. 5.3(2));
2. **Decision:** a written, reasoned decision within four (4) weeks of receipt, including whether the complaint will be processed and, if so, the final ruling (Art. 5.3(4));
3. **Extension:** the four-week period may be extended once, in writing, by a further four (4) weeks (Art. 5.3(5)); and
4. **Records:** all complaints, decisions and outcomes are recorded and retained, and form part of the reports to the CGA (§16).

12.3 Alternative Dispute Resolution

Where a complaint cannot be resolved through the internal procedure, the player may escalate it, free of charge, to an independent Alternative Dispute Resolution (ADR) provider that is certified by the CGA and established in Curaçao. The ADR provider is a separate entity from the Operator, operates its own website, and reviews the evidence submitted by both parties to determine whether the matter requires mediation or adjudication (Art. 5.3(6)-(7)).

The Operator bears all costs of the ADR process, which is provided at no cost to the player, and treats the outcome as binding on the Operator. The Operator has contracted the following CGA-certified ADR provider, selected from the official list published by the CGA: **[contracted ADR provider - name and website]**. The ADR procedure and the provider's contact details are published on the Operator's website, and cases referred to the provider are handled within ninety (90) days.

12.4 Governing Law and Jurisdiction

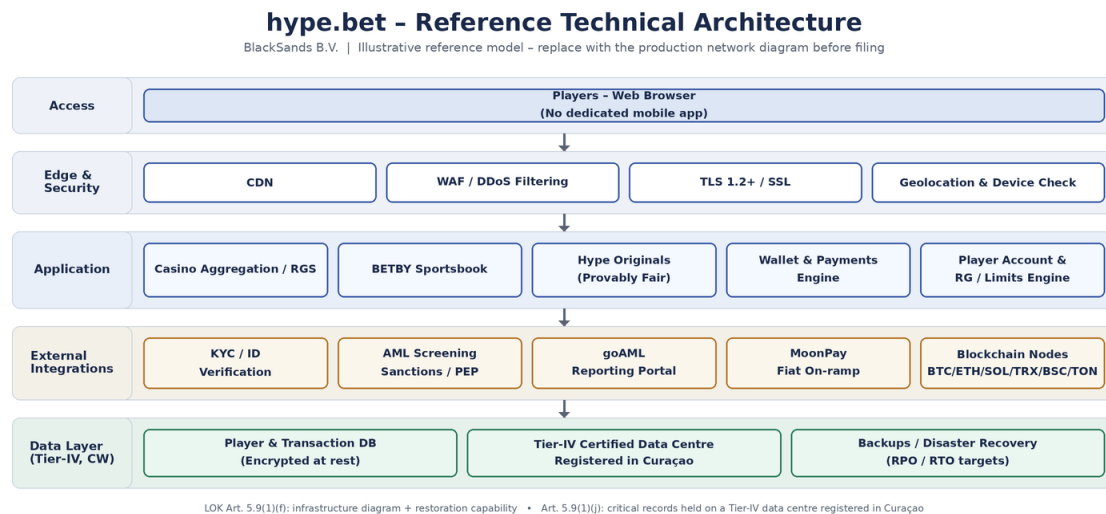
The gaming agreement between the Operator and the player is subject to Curaçao law, and disputes relating to it are brought before the Curaçao courts (Art. 5.5). This clause is reflected in the general terms and conditions (Appendix K).

13. Technical Infrastructure

This section satisfies Article 5.9(1)(f) and supports Article 5.9(1)(j).

13.1 Infrastructure Diagram

The diagram below sets out the reference architecture of the gaming operation. It is illustrative and must be replaced with the production network diagram before filing.



13.2 Hosting Environment

Critical player, gaming and financial records are held on a server of a Tier-IV certified data centre registered in Curaçao (Art. 5.9(1)(j)). The Operator additionally Tier-IV data center with monitored backup systems. The certified data-centre operator is Flutter Networks N.V a limited liability company, duly organized according to the Laws of Curaçao, with registration number 161318.

13.3 Security Controls

Security controls include:

- Multi-factor authentication for administrative access;
- Encryption in transit and at rest;
- Vulnerability management and periodic penetration testing;
- Role-based access control, logging and monitoring; and
- Independent security testing, including penetration testing carried out at least annually by an external security firm, with findings tracked through to remediation.

14. Business Continuity and Disaster Recovery

This section supports the restoration-capability requirement of Article 5.9(1)(f).

14.1 Incident Classification

Severity	Description
Minor	Limited impact; no material effect on players, funds or data; handled within normal operations.
Major	Significant degradation of service, partial outage, or potential data/security impact requiring escalation.
Critical	Loss of service, fund or data integrity risk, or security breach - triggers DR and 24-hour CGA incident reporting (§16).

14.2 Disaster Recovery

Disaster-recovery procedures include data restoration from backups, system failover, and defined internal and external communication protocols, with restoration capability for technical emergency situations affecting the operation (Art. 5.9(1)(f)).

14.3 Recovery Objectives

Objective	Target
Recovery Time Objective (RTO)	4 hours for critical player-facing, wallet and payment services
Recovery Point Objective (RPO)	15 minutes (near-continuous replication of transactional data)

15. Record Keeping

This section implements Article 5.11 and supports Article 5.9(1)(j).

The Operator maintains complete and accessible digital records, including:

- Player identities and KYC documentation;
- Gaming transactions and bet/outcome data;
- Financial transactions (deposits, withdrawals, balances);
- Complaints and their outcomes;
- Responsible-gaming interventions and self-exclusions;
- AML/CFT reviews and reports; and
- Regulatory filings and correspondence.

Records are kept so that the rights and obligations of the Operator and the player are clear at all times (Art. 5.11(2)), are retained for the legally prescribed period, and are held on the Tier-IV data centre referred to in §13.2. Annual financial statements are submitted to the CGA by 30 June of the following calendar year (Art. 5.11(3)), and interim financial reports are provided where required.

16. Incident and Regulatory Reporting

This section implements Article 5.10.

Report	Trigger / contents	Deadline
Incident report	Security breaches affecting player data/game details; failure/loss/damage to equipment or software causing loss of games; (attempted) fraud or criminal behaviour; other serious threats to the integrity of the operation (Art. 5.10(5))	Within 24 hours of the incident (Art. 5.10(6))
Amendment report	Changes to this Operations Manual in the past period, with the updated Manual attached (Art. 5.10(4))	Twice yearly - by 15 June and 15 January
Gambler transaction report	Total amounts and nature of crediting/debiting of gaming accounts; payment-instrument and (non-identifying) account identifiers per domain/application (Art. 5.10(7))	As specified by the CGA
Annual financial statements	Audited/financial statements for the prior year (Art. 5.11(3))	By 30 June

The Compliance Officer is responsible for preparing and submitting these reports, using CGA templates where provided, and for retaining evidence of submission.

17. Training Program

This section implements the permanent-education requirement of Article 5.9(4).

The Operator provides annual permanent education to persons working in the field of games of chance, delivered according to the knowledge and experience expected for each role. The program covers, at a minimum:

- Mental well-being;
- Anti-bribery;
- Crime prevention;
- Responsible gaming;
- Anti-money laundering and counter-terrorist financing;
- Communication with players; and
- Responsible advertising.

Training is role-based, completion is recorded, and the training matrix is maintained by Compliance (Appendix H).

18. Review and Updates

This Operations Manual is reviewed:

- At least annually; and
- Whenever there is a material change to operations, systems, ownership, products or regulatory requirements.

Material changes are reflected in a new version, approved by the Managing Director, and notified to the CGA through the next amendment report (and immediately where an incident report is required). Superseded versions are retained for audit purposes.

Appendix I - Domain Register

Domain / application	Type	Status
www.hype.bet	Primary website	Active

End of Operations Manual - hype.bet - BlackSands B.V. - Version 1.0