

**OXILIUM N.V.**  
**OPERATIONS MANUAL**

For Bahisbey.com and associated approved domain aliases

| Field             | Details                                             |
|-------------------|-----------------------------------------------------|
| Company           | Oxilium N.V.                                        |
| Brand / platform  | Bahisbey.com and associated approved domain aliases |
| Document title    | Operations Manual                                   |
| Jurisdiction      | Curaçao                                             |
| Licence reference | OGL/2024/1601/0909                                  |
| Version           | Version 1.1                                         |
| Effective date    | 30/07/2026                                          |
| Document status   | Approved                                            |
| Classification    | Internal / Regulatory                               |
| Document owner    | MLRO / Compliance Officer                           |
| Prepared for      | Management Review and Approval                      |
| Approved by       | 30/07/2026                                          |
| Approval date     | 30/07/2026                                          |
| Next review date  | 30/06/2027                                          |

## **Table of Contents**

1. Introduction and Document Control
2. Company, Licence and Operating Model
3. Games of Chance Offered and Product Scope
4. Payment Possibilities and Player Credit Controls
5. Quality Monitoring, Testing and Certification Evidence
6. Player Data, Records and Retention
7. Player-Facing Website and Visual Elements
8. Access Controls and Excluded / Banned Persons
9. Responsible Gaming Implementation Interface
10. Terms and Conditions
11. Player Complaints and Dispute Settlement
12. Technical Infrastructure and Business Continuity
13. AML/CFT/CPF Operational Interface
14. Sanctions and Targeted Financial Sanctions
15. Supplier and Outsourcing Management
16. Reports, Incidents and Regulatory Availability
17. Training and Awareness
18. Registers and Evidence Schedule
19. Implementation Action Tracker

## 1. Introduction and Document Control

### 1.1 Purpose of this Operations Manual

This Operations Manual describes the operational, technical, compliance and governance framework through which Oxilium N.V. conducts, controls and evidences its remote gaming operation under the Bahisbey brand. It describes the control environment applicable to Bahisbey.com and associated approved domain aliases, while leaving unconfirmed factual matters marked as TBC or Action Required.

The Manual explains how the Company operates and controls games of chance, payment methods, player credit restrictions, software and technical infrastructure, quality monitoring, player data, website disclosures, access controls, responsible gaming, Terms and Conditions, complaints, AML/CFT/CPF, sanctions, outsourcing, regulatory reporting, training and evidence maintenance.

This Manual does not replace standalone Company policies. It operates as the central operational document linking those policies to the Company's day-to-day operating model, supplier arrangements, registers, evidence files and escalation routes.

### 1.2 Legal and Regulatory Basis

This Manual has been prepared to support the Company's obligations as a Curaçao-licensed remote gaming operator, including the requirement to maintain an operations manual describing the operator's games, payment possibilities, technical infrastructure, responsible gaming implementation, Terms and Conditions, dispute settlement and regulatory access to critical records.

The Manual also supports operational compliance with requirements relating to player protection, responsible gaming, fair and verifiable gaming operations, AML/CFT/CPF, sanctions and targeted financial sanctions, complaint handling and ADR, information security, outsourcing, recordkeeping, incident management and regulatory inspection readiness.

Where this Manual refers to a regulatory requirement, licence condition, regulator expectation or operational control, the Company must ensure that the underlying evidence is held in the relevant compliance file before the Manual is treated as final.

### 1.3 Regulatory Mapping to Operations Manual Requirements

The Company shall maintain this Manual in a manner that demonstrates how its remote gaming operation addresses the principal operations manual requirements under applicable Curaçao law, the Company's licence conditions and applicable CGA requirements. The mapping below is included as an internal control and evidence tool to show where the relevant operational, compliance, governance and recordkeeping topics are addressed in this Manual and where supporting evidence should be maintained.

| Requirement / topic                                                                                     | Manual section and evidence location                                                                                       |
|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Games of chance, product scope, rules, bet and payout limits, software and outcome-determining elements | Sections 3 and 5; product register, game list, game rules, RNG / game certificates and testing register.                   |
| Payment possibilities, payment ownership, withdrawal controls and prohibition on player credit          | Section 4; payment-method register, payment flows, provider agreements, reconciliation records and no-credit confirmation. |

|                                                                                                         |                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Responsible gaming implementation, limits, cooling-off, self-exclusion and marketing suppression        | Sections 8, 9, 10 and 17; responsible gaming tool configuration, testing evidence, screenshots, training records and case register.               |
| Current Terms and Conditions, player agreement, rules, complaints, governing law and dispute settlement | Sections 7, 10 and 11; current T&Cs, acceptance evidence, archive, complaint procedure and ADR disclosure.                                        |
| Digital critical player, gaming and financial records and regulatory availability                       | Sections 6, 12, 16 and 18; recordkeeping evidence, export capability, Tier-IV Curaçao data centre evidence and CGA availability mechanism.        |
| AML/CFT/CPF, sanctions and targeted financial sanctions operational controls                            | Sections 13 and 14; AML/KYC policies, Sumsb configuration, transaction monitoring, goAML workflow, sanctions screening and frozen asset register. |
| Incidents, amendments, regulatory reports, complaints reports and regulatory requests                   | Sections 11 and 16; reporting calendar, incident register, complaint register, regulatory request log and evidence production log.                |
| Training and awareness for relevant personnel                                                           | Section 17; training calendar, training materials, attendance records and effectiveness review.                                                   |
| Supplier and outsourcing oversight                                                                      | Section 15; supplier register, due diligence, agreements, SLAs, responsibility matrix, monitoring and exit plans.                                 |

## 1.4 Scope

This Manual applies to Oxilium N.V., Bahisbey.com, associated approved domain aliases, the player account and wallet environment, sportsbook, casino, slots, live casino, virtual sports, jackpot and bingo products where active, fiat payment methods, crypto payment arrangements, KYC / AML systems, sanctions screening, responsible gaming tools, complaints and ADR arrangements, technical infrastructure, suppliers, outsourced service providers and records maintained for regulatory compliance.

This Manual applies to personnel, officers, senior managers, compliance staff, customer support personnel, payment and technical owners, supplier relationship owners and any outsourced personnel or suppliers whose functions materially affect the licensed operation.

This Manual does not make country-specific representations regarding the market focus of the platform unless such representation is confirmed in approved Company documents, licence filings, Terms and Conditions or regulator-facing disclosures.

## 1.5 Relationship with Other Company Policies

This Manual must be read together with the Anti-Money Laundering and Terrorist Financing Policy, KYC Policy, Information Security Policy, Cryptocurrency Risk Management Policy, Responsible Gaming Policy, Complaints Policy, Terms and Conditions, Privacy Notice, sanctions and targeted financial

sanctions procedures, transaction monitoring procedures, supplier agreements and any other operating procedure or register maintained by the Company.

Where a matter is addressed in detail in a standalone policy, this Manual describes the operational interface, ownership, evidence requirements and unresolved Company confirmations rather than duplicating every policy provision. Where a standalone policy is outdated, incomplete or inconsistent with the actual operating model, the relevant item is marked as TBC / Action Required.

If a conflict exists between this Manual and a standalone policy, the MLRO / Compliance Officer must review the inconsistency, determine the appropriate amendment and escalate the issue to senior management or the Board where material.

## **1.6 Evidence Reliance Statement**

This Manual has been prepared on the basis of Company documents, internal policies, operational confirmations and regulatory materials available as of TBC. Where a document, factual confirmation, supplier record, licence document, system configuration, technical evidence or operational confirmation remains outstanding, the relevant item is marked as TBC or Action Required.

No unconfirmed item should be treated as final, approved, implemented or regulator-ready until the relevant evidence has been obtained, reviewed and stored in the Company's compliance records. The Company must not rely on unsupported verbal statements, informal supplier messages or screenshots without context as final regulatory evidence.

Each evidence item requested in this Manual should be provided by the Company or relevant supplier and stored in the evidence repository identified in Section 18.

## **1.7 Hierarchy and Conflicts**

If there is any conflict between this Manual and applicable law, licence conditions, CGA requirements, AML/CFT/CPF requirements, sanctions obligations or any binding regulatory instruction, the applicable legal or regulatory requirement shall prevail.

If there is any conflict between this Manual and a supplier agreement, the Company must assess whether the supplier arrangement creates a regulatory, operational, data-protection, business-continuity or player-protection gap. A supplier agreement must not be used to limit the Company's regulatory responsibilities unless legally permissible and approved by the relevant regulator.

Where a conflict is identified, the MLRO / Compliance Officer must record the issue, assign an owner, determine whether immediate interim controls are required and enter remediation into the Implementation Action Tracker.

## **1.8 Ownership, Approval and Review**

The MLRO / Compliance Officer is the primary owner of this Manual and is responsible for maintaining the Manual, coordinating updates, tracking unresolved TBC items, reviewing compliance-sensitive amendments, coordinating evidence collection and escalating Critical gaps.

The Board and senior management retain ultimate responsibility for approving the Manual and ensuring that the Company has adequate systems, controls, personnel, supplier arrangements and evidence to support the matters described in it.

The Manual shall be reviewed at least annually and following material changes to licence status, products, payment methods, crypto assets or networks, suppliers, infrastructure, responsible gaming tools, complaints or ADR arrangements, technical incidents, audit findings, regulatory requests or changes to applicable law or regulator expectations.

## 1.9 Treatment of TBC Items

Any item marked TBC must be treated as unresolved until the relevant confirmation, document or evidence has been obtained. Any item marked TBC / Action Required must be treated as requiring positive remediation, amendment, implementation or provision of documents before the relevant section can be considered final.

Critical TBC items must be entered into the Implementation Action Tracker and escalated to senior management or the Board if they remain unresolved before final approval. The Company should not remove a TBC marker unless the relevant evidence is provided and the Manual text has been updated accordingly.

Where a TBC item cannot be closed immediately, the Company should document an interim control, deadline, responsible owner and risk acceptance decision where appropriate.

## 1.10 Finalisation Status

This Manual is currently a Working Draft for Company review and confirmation. It should not be treated as final, Board-approved or regulator-ready until all Critical TBC items have been closed or formally escalated; the current licence certificate and licence conditions have been confirmed; the current Terms and Conditions have been obtained and reviewed; ADR disclosure has been confirmed; the Tier-IV Curaçao data centre arrangement has been evidenced; critical supplier agreements and responsibility matrices have been obtained; product and game certification evidence has been reviewed; and the Board or authorised approving body has approved the Manual or approved it subject to documented conditions.

### Records and Evidence

| Record / evidence item      | Status                                                                                                      |
|-----------------------------|-------------------------------------------------------------------------------------------------------------|
| Current licence certificate | Available                                                                                                   |
| Licence conditions          | Indefinite license – current certificate and licence conditions to be retained in license file              |
| Evidence repository         | Oxilium N.V. compliance evidence folder                                                                     |
| Version history             | Version 1.0 – initial company review draft dated 22/06/2026<br>Version 1.1 – Final version dated 30/07/2026 |
| Board approval record       | Approved by senior management and retained with company records                                             |

## 2. Company, Licence and Operating Model

### 2.1 Company Overview

Oxilium N.V. is the company responsible for the operation of Bahisbey.com and associated approved domain aliases. The Company is treated in this Manual as the licensed operator responsible for the player-

facing platform, player accounts, games, payments, compliance framework, responsible gaming tools, complaints process, supplier oversight, regulatory reporting and regulatory recordkeeping.

The Company must maintain up-to-date corporate records, including incorporation evidence, company extract, registered office, directors and officers, UBO or ownership records, management appointments, licence certificate, licence conditions and approved domain records. These records must be retained in the corporate and licence evidence file.

## **2.2 Licence Status**

The Company's internal AML/CFT/CPF Policy identifies Oxilium N.V. as holder of Gaming Licence No. OGL/2024/1601/0909.

The Company shall not rely on the licence reference as final regulatory evidence unless the current licence certificate and applicable licence conditions have been obtained, reviewed and stored. The licence file must identify the licence holder, licence number, effective date, scope, approved products, approved domains, conditions, reporting obligations, renewal dates and any restrictions relevant to the operation.

## **2.3 Brand, Platform and Domains**

The Company operates under the Bahisbey brand. For the purposes of this Manual, all references to the platform mean Bahisbey.com and associated approved domain aliases.

The Company shall maintain a current domain and alias register identifying the primary domain, approved aliases, redirects, mirror or mobile interfaces, licence display, Terms and Conditions URL, Privacy Notice URL, Responsible Gaming page, Complaints / ADR page, payment page, bonus / promotion pages and status of each domain or interface.

No domain, mirror, redirect or player-facing interface should be used for player acquisition, registration, deposits or gameplay unless it has been reviewed for consistency with the Company's licence, Terms and Conditions, responsible gaming disclosures, complaint disclosures, payment disclosures and regulatory obligations.

## **2.4 Operating Model Summary**

Based on available confirmations, the operating model includes Digitain as platform / games / sportsbook provider, Bank Havale and Papara for fiat and bank transfers payments, Spinmatic Limited as payment agent, CoinPayments / UAB Star Ventures for crypto payment processing, Sumsu for KYC / AML, Curaçao VPS Hosting subject to role and sufficiency confirmation, EGIS-FZCO as ADR provider, internally managed customer support and referral sites for traffic.

This operating model summary must be reconciled against written contracts, supplier due diligence files, technical diagrams, data flow maps, product registers, payment flow documentation, crypto flow documentation and player-facing website screenshots. Where supplier arrangements or payment flows differ from this summary, the Manual must be updated and the discrepancy recorded.

## **2.5 Senior Management and Key Functions**

Based on operational confirmations, Christiana Ilia is CEO and CFO and Justice Nwankwo handles MLRO / Compliance Officer functions and related compliance, responsible gaming and complaints functions, subject to formal appointment evidence and scope confirmation.

The Company must maintain a responsibility matrix identifying the Board, CEO, CFO, MLRO / Compliance Officer, responsible gaming owner, complaints owner, payments owner, technical owner, supplier owner, data protection or information security owner and any deputy or backup arrangements.

IT, security, supplier technical support and incident functions may be operationally supported by Digitain or other suppliers, but Oxilium N.V. retains ultimate responsibility for the adequacy of controls and regulatory compliance.

## 2.6 Governance and Accountability

The Board and senior management retain ultimate responsibility for licence compliance, player protection, responsible gaming, AML/CFT/CPF, sanctions, complaints, payment controls, crypto controls, information security, supplier risk, regulatory reporting, training and maintenance of this Manual.

The use of suppliers does not transfer regulatory responsibility away from Oxilium N.V. Supplier arrangements must therefore include appropriate oversight rights, incident notification, evidence provision, audit support, regulatory cooperation, data availability and exit arrangements.

Senior management must ensure that sufficient resources, tools, access rights, training and evidence repositories are available for the MLRO / Compliance Officer and other control owners to perform their duties.

## 2.7 Internal Escalation

The Company shall maintain clear escalation routes for licence matters, AML/CFT/CPF concerns, unusual or suspicious transactions, sanctions matches, KYC / EDD failures, payment holds, crypto alerts, responsible gaming concerns, complaints, ADR matters, technical incidents, supplier failures, data incidents and CGA or FIU requests.

Escalation records must identify the matter, source, date and time, responsible owner, decision, evidence reviewed, action taken, reporting assessment and closure status. Where an issue is material or time-sensitive, escalation to senior management must occur without delay.

## Records and Evidence

| Record / evidence item                        | Status                                                                  |
|-----------------------------------------------|-------------------------------------------------------------------------|
| Current company extract                       | Available                                                               |
| Corporate registration and registered address | 165075, Dr. M. J. Hugenholtzweg 25, Willemstad, Curacao                 |
| UBO / ownership records                       | Available                                                               |
| Current licence certificate                   | Indefinite license – current certificate to be retained in license file |
| License conditions                            | License conditions to be retained in license file                       |
| CGA portal status                             | Active                                                                  |
| Approved domain / alias list                  | Bahisbey.com                                                            |
| MLRO / Compliance Officer appointment         | MLRO / Compliance Officer appointed                                     |
| Internal responsibility matrix                | Available                                                               |

|                                |           |
|--------------------------------|-----------|
| Supplier responsibility matrix | Available |
|--------------------------------|-----------|

### 3. Games of Chance Offered and Product Scope

#### 3.1 Purpose and Product Scope

This section describes the games of chance and product verticals offered or intended to be offered through Bahisbey.com and associated approved domain aliases and identifies required evidence for product scope, rules, software, outcome-determining elements, bet limits, payout limits, supplier role and certification.

Based on operational confirmations, the platform includes or is intended to include sportsbook, casino, slots, live casino, virtual sports, jackpot / progressive products and bingo. This must be reconciled against the final product register, game list, supplier list, certification evidence and current player-facing website.

#### 3.2 Product Register

The Company shall maintain a product register identifying all active product verticals and games. The register must be sufficiently detailed to allow the Company, auditor, ADR provider or regulator to identify what is offered to players, who supplies it, how outcomes are determined, what limits apply and what evidence supports fairness and certification.

The product register shall include product vertical, product or game name, supplier, aggregator if any, software version, launch date, removal or suspension date, game category, rules location, minimum bet, maximum bet, maximum payout, jackpot mechanics where applicable, RNG / fairness evidence, certification evidence, product owner, status and evidence storage location.

#### 3.3 Active, Approved and Intended Product Classification

For regulatory and evidence purposes, the Company shall classify each product vertical and game as active, approved but not active, suspended, removed or planned / not yet launched. The Manual, product register, Terms and Conditions, player-facing rules and website screenshots must not imply that a product is active unless it is actually available to players and supported by supplier, testing and certification evidence.

Where a product is planned or intended but not yet active, the product register must identify the intended launch status, required approvals, supplier evidence, testing evidence, certification evidence, Terms and Conditions updates and any regulatory notification or approval assessment.

#### 3.4 Sportsbook

Sportsbook records shall identify the supplier, odds feed or odds-generation arrangement, event and market coverage, bet acceptance rules, market suspension rules, settlement process, void and cancellation rules, maximum stake, maximum payout, rejection rules, cash-out where applicable, dispute and resettlement rules, reporting capability, audit log capability and supplier escalation process.

Sportsbook operations must be supported by player-facing rules that explain how bets are accepted, settled, voided, cancelled, amended or refused. Any settlement correction must preserve the original settlement record, reason for correction, supplier evidence, approval and player communication.

### 3.5 Casino, Slots and Live Casino

Casino, slots and live casino records shall identify supplier, title, category, RNG or live-dealer nature, RTP or equivalent return information, rules, payout table, minimum and maximum bet, maximum payout, certification evidence, version and status.

For live casino, the Company must retain evidence of supplier/studio arrangement, operating rules, game provider identity, player rules, complaint escalation, settlement records and incident procedures. Where live casino is provided by a third-party supplier, the Company remains responsible for ensuring that supplier evidence can be produced when required.

### 3.6 Virtual Sports, Jackpot and Bingo

Virtual sports must identify supplier, rules, event-generation and outcome-determining mechanism, odds / payout structure, certification evidence and settlement logic. Where the product uses RNG or simulated events, the relevant testing evidence must be retained.

Jackpot products must document contribution, prize pool, trigger, payout, display, reset, malfunction rules, funding, award logs and supplier responsibility. Bingo must document draw mechanism, card generation, winning patterns, prize rules, session rules, audit logs, certification and player-facing rules.

### 3.7 Software and Outcome-Determining Elements

The Company shall identify and evidence platform software, game software, RNG, sportsbook settlement feed, virtual sports event generator, jackpot trigger, bingo draw mechanism, live casino supplier systems, wallet integration, bonus engine, reporting module and audit tools.

No system, product or outcome-determining element should be described as certified, approved, tested or compliant unless written evidence is held in the certification register or supplier evidence file.

### 3.8 Bet Amounts, Payouts and Player Disclosure

The Company shall maintain clear records of minimum and maximum bet amounts, maximum payouts, jackpot rules, bonus-related limits and currency-specific limits. These must match the platform configuration and the player-facing Terms and Conditions or game rules.

Player-facing rules must disclose game rules, bet placement, settlement, winning conditions, payout, void / cancellation, malfunction, bonus restrictions, jackpot rules and complaint route. Where rules are hosted or supplied by a supplier, the Company must retain evidence of the version made available to players.

### 3.9 Product Changes

Material product changes, including new product verticals, new suppliers, jackpot mechanisms, sportsbook settlement changes, game rules, bet limits, payout limits, bonus mechanics or player-facing disclosures, shall be reviewed before launch for impact on Terms and Conditions, product rules, AML controls, responsible gaming controls, supplier register, certification register, this Manual and regulatory reporting obligations.

Product changes must be recorded in a product change register with description, owner, risk assessment, testing evidence, approval, launch date, player-facing disclosure update and evidence location.

### Records and Evidence

| Record / evidence item | Status |
|------------------------|--------|
|------------------------|--------|

|                                          |                                                                                                                                                                                 |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Product register                         | Maintained by the Company and platform provider and updated with all active product verticals and suppliers                                                                     |
| Full active game list                    | Maintained by the Company and platform provider and updated daily                                                                                                               |
| Supplier list by product vertical        | Digitain platform, sportsbook, casino aggregation and related technical services                                                                                                |
| Sportsbook rules and settlement evidence | Digitain odds and settlement system                                                                                                                                             |
| Casino / slots / live casino rules       | Provided by Game suppliers                                                                                                                                                      |
| Virtual sports and jackpot evidence      | Provided by Game suppliers                                                                                                                                                      |
| Bingo rules and certification            | Provided by Game suppliers                                                                                                                                                      |
| RNG certificates                         | Provided by Digitain and retained with game certification records                                                                                                               |
| Game certificates                        | Provided by Digitain and retained with game certification records                                                                                                               |
| Bet and payout limits                    | Available                                                                                                                                                                       |
| Player-facing rule screenshots           | Available                                                                                                                                                                       |
| Product change register                  | Changes to products, suppliers, game rules, bet limits, payout limits or certifications require review by Compliance, Management and implementation from Digitain before launch |

## 4. Payment Possibilities and Player Credit Controls

### 4.1 Purpose and General Payment Principles

This section describes payment methods, fiat and crypto payment flows, withdrawal controls, payment ownership controls, reconciliation and the prohibition on player credit. Payment arrangements must be controlled, documented, auditable and consistent with the Terms and Conditions, AML/CFT/CPF Policy, KYC Policy and Cryptocurrency Risk Management Policy.

Only approved payment methods may be used. Deposits and withdrawals must link to registered player accounts. Payment methods must belong to the player. Third-party payments are prohibited unless a lawful, documented and approved exception exists. Withdrawals may be subject to KYC, EDD, AML, sanctions, fraud, payment ownership and responsible gaming checks.

## 4.2 Approved Payment Methods

Current confirmations identify Bank Havale / bank transfers facilitated by Maldo Limited, Papara facilitated by Maldo Limited, Spinmatic Limited as payment agent, CoinPayments / UAB Star Ventures for crypto, and USDT TRC, USDT ERC and USDC ERC as crypto assets/networks.

The Company must maintain a payment-method register identifying all deposit and withdrawal methods, provider names, currencies, limits, processing times, ownership checks, supported jurisdictions, provider restrictions, fees, reconciliation arrangements, active status and evidence location.

## 4.3 Fiat Payments and Payment Agent

For fiat methods, the Company shall document provider identity, legal relationship, deposit flow, withdrawal flow, settlement, reconciliation, currencies, limits, ownership checks, chargeback and reversal handling, suspicious transaction escalation, sanctions interface and incident route.

Spinmatic Limited's role as payment agent must be evidenced by agreement, scope, accounts used, responsibilities, settlement flow, reconciliation process, AML cooperation obligations, sanctions cooperation obligations, access to records, termination rights and incident escalation.

## 4.4 Crypto Payments

The Company shall maintain evidence for CoinPayments / UAB Star Ventures covering legal identity, agreement, supported assets and networks, wallet custody model, wallet generation, deposit and withdrawal flow, transaction monitoring, sanctions and wallet-risk screening, reporting access, incident escalation and continuity arrangements.

The current Cryptocurrency Risk Management Policy must be updated to reflect all active crypto assets and networks, including USDT TRC, USDT ERC and USDC ERC, and any additional assets or networks actually offered to players.

## 4.5 Deposit and Withdrawal Flow

Deposit and withdrawal flows must identify login and account checks, payment method selection, limits, responsible gaming limits, KYC triggers, AML triggers, sanctions checks, provider processing, crediting or execution, failure handling, reconciliation and retained records.

Crypto flows must additionally include asset and network selection, warnings for unsupported networks, blockchain confirmations, transaction hash recording, wallet ownership checks, wallet-risk screening, wallet sanctions review, unsupported asset or network handling and error resolution.

## 4.6 Payment Ownership and Third-Party Payments

The Company shall verify that payment methods belong to the registered player. Ownership evidence may include bank statement, payment provider account evidence, card or account holder confirmation, crypto wallet ownership evidence, transaction history or proof of control.

Suspected third-party payment activity must be escalated to Compliance and may require EDD, payment hold, account restriction, refund assessment, suspicious activity review or reporting assessment. The Company must retain the evidence reviewed and the decision taken.

## 4.7 No Player Credit

The Company shall not provide credit, loans, overdrafts, deferred payment arrangements or equivalent credit facilities to players unless expressly permitted by law, licence conditions and internal policy.

Players must not be allowed to place bets without sufficient available balance. Failed deposits must not create usable balance. Reversed payments, negative balances and balance discrepancies must be escalated, documented and corrected in accordance with approved procedures.

#### 4.8 Payment Holds and Reconciliation

Payment holds may apply for incomplete KYC, EDD, sanctions alerts, payment ownership concerns, responsible gaming restrictions, fraud concerns, duplicate accounts, chargebacks, provider incidents, crypto wallet-risk alerts or regulatory instruction.

Reconciliation shall compare platform records, provider records, payment-agent records, bank records and crypto records. Reconciliation exceptions must be recorded, investigated, assigned to an owner and closed with evidence.

#### 4.9 Player-Facing Payment Disclosure

Player-facing payment disclosures must accurately describe available payment methods, currencies, crypto assets and networks, limits, processing times, KYC and AML checks, payment ownership requirements, third-party payment prohibition, fees, payment holds, unsupported crypto network risks and complaint routes.

Payment disclosures must be consistent across the website, payment pages, Terms and Conditions, support scripts and any affiliate or marketing material controlled by the Company.

#### Records and Evidence

| Record / evidence item                        | Status    |
|-----------------------------------------------|-----------|
| Active payment-method register                | Available |
| Bank Havale / bank transfer flow              | Available |
| Papara / bank transfer flow                   | Available |
| Spinmatic Limited agreement                   | Available |
| CoinPayments / UAB Star Ventures agreement    | Available |
| Updated Cryptocurrency Risk Management Policy | Available |
| Deposit / withdrawal flows                    | Available |
| Reconciliation records                        | Available |

### 5. Quality Monitoring, Testing and Certification Evidence

#### 5.1 General Quality Monitoring Principles

The Company shall maintain quality monitoring arrangements to verify that the operation remains fair, reliable, secure, auditable and consistent with player-facing rules. Monitoring shall cover platform functionality, game and sportsbook operation, outcome-determining elements, payment integrations,

crypto, KYC / AML, sanctions, transaction monitoring, responsible gaming, wallet, reporting, records and information security.

Quality monitoring must be evidence-based. Supplier statements must be supported by certificates, test reports, integration evidence, logs, screenshots, configuration exports, incident reports or formal written confirmations retained in the relevant evidence file.

## **5.2 Testing and Certification Register**

The Company shall maintain a testing and certification register identifying the system, product or control tested; supplier; testing body; test date; certificate or report reference; standard or scope; outcome; exceptions; remediation items; next review date; and evidence storage location.

No system, game, RNG, sportsbook settlement mechanism, virtual sports event generator, jackpot mechanism, bingo draw mechanism, payment integration or compliance tool should be described as certified, approved or tested unless written evidence is held.

## **5.3 Product, Game and Outcome Testing**

Evidence may include game certificates, RNG certificates, laboratory reports, supplier certificates, technical compliance statements, integration test records, RTP / PAR sheets, jackpot testing, bingo draw testing, sportsbook settlement testing and product launch approval records.

Outcome-determining elements must be identified and controlled. Any change to an outcome-determining element must be reviewed for testing, certification, player disclosure, supplier responsibility and regulatory reporting impact.

## **5.4 Platform, Payment and Crypto Testing**

Platform testing should cover registration, account management, wallet balances, game access, product availability, payment integration, responsible gaming tools, complaints interface, reporting tools, audit logs and data exports.

Payment testing should cover successful and failed deposits and withdrawals, payment ownership checks, KYC / AML / sanctions holds, responsible gaming interactions, provider reporting, reconciliation and exception handling. Crypto testing should cover supported and unsupported networks, wallet generation, blockchain confirmations, transaction hashes, wallet ownership, wallet-risk alerts and unsupported asset handling.

## **5.5 KYC / AML, Sanctions and Responsible Gaming Testing**

The Company shall test Sumsub configuration, identity verification, proof of address, age verification, sanctions screening, PEP screening, adverse media screening, ongoing rescreening, case management, transaction alerts, escalation workflows, customer risk scoring, withdrawal holds and reporting capability.

Responsible gaming testing shall cover deposit limits, loss limits, session limits, reality checks, cooling-off, self-exclusion, account restriction, marketing suppression and duplicate-account indicators. Testing evidence must be retained.

## **5.6 Information Security, Backup and Supplier Assurance**

The Company shall maintain evidence of vulnerability assessment, penetration testing where applicable, access-control review, privileged access review, MFA testing, logging, backup restoration testing, incident response testing and supplier security evidence review.

Supplier assurance shall be supported by agreements, SLAs, certificates, audit reports, business continuity evidence, disaster recovery evidence, incident escalation contacts and regulatory cooperation obligations.

## 5.7 Incident-Based and Change-Based Testing

Incidents, complaints, audit findings or supplier failures may require targeted testing. Material changes to products, suppliers, payment methods, crypto assets, KYC / AML, sanctions, responsible gaming tools, platform releases, hosting or reporting must be tested, approved and documented before release where relevant.

### Records and Evidence

| Record / evidence item                       | Status    |
|----------------------------------------------|-----------|
| Testing and certification register           | Available |
| Product and game certification evidence      | Available |
| RNG certificates                             | Available |
| Platform testing evidence                    | Available |
| Payment and crypto testing evidence          | Available |
| Sumsb configuration and testing evidence     | Available |
| Responsible gaming tool testing evidence     | Available |
| Vulnerability / penetration testing evidence | Available |
| Backup / restoration testing evidence        | Available |

## 6. Player Data, Records and Retention

### 6.1 General Recordkeeping Principles

The Company shall maintain accurate, complete, time-stamped, attributable, access-controlled and retrievable records for player accounts, gaming transactions, financial transactions, AML / KYC, sanctions, responsible gaming, complaints, incidents, supplier evidence and regulatory reporting. Records must be protected against unauthorised alteration and loss.

The Company must be able to reconstruct relevant player activity, gaming activity, payment activity, compliance decisions, complaint history and regulatory responses. Records shall be retained for the required period and made available for review, audit, ADR or regulatory inspection where required.

### 6.2 Categories of Player and Account Data

Player data may include legal name, date of birth, nationality, address, email, mobile number, registration country, account identifier, IP and device data, KYC documents, payment method information, crypto wallet information, responsible gaming settings, complaint history and support communications.

Player account records shall evidence account creation, registration details, Terms and Conditions acceptance, KYC status, risk rating, restrictions, duplicate review, self-exclusion or cooling-off, payment methods, suspension and closure.

### **6.3 Gaming and Financial Transaction Records**

Gaming records should include player identifier, product, game or event, round or bet ID, timestamp, stake, odds, outcome, payout, void / cancellation / resettlement, bonus involvement, jackpot contribution or award, supplier reference and audit logs.

Financial records should include transaction ID, method, provider, payment agent, amount, currency, status, provider reference, wallet reference, blockchain transaction hash, ownership status, KYC / AML / sanctions / responsible gaming holds, reconciliation status and manual adjustments.

### **6.4 AML / KYC, Sanctions, Responsible Gaming and Complaints Records**

AML / KYC records include CDD, EDD, identity verification, sanctions, PEP, adverse media, customer risk assessment, source of funds, source of wealth, payment ownership, crypto wallet ownership, transaction monitoring alerts, internal suspicious reports and FIU submissions.

Sanctions records include onboarding and rescreening results, potential match reviews, true match decisions, frozen asset register, authority reports and communications. Responsible gaming records include limits, reality checks, cooling-off, self-exclusion, marketing suppression, interactions, escalations and complaints. Complaint and ADR records must evidence intake, investigation, response, escalation and outcome.

### **6.5 System Logs and Access Controls**

The Company shall maintain system logs and audit trails for logins, admin access, account status changes, balance changes, payment approvals, KYC / AML decisions, sanctions decisions, responsible gaming changes, bonus adjustments, complaints, configurations and incidents.

Access to records must be controlled by role-based permissions, MFA where appropriate, least privilege, periodic access reviews, supplier access restrictions and confidentiality obligations.

### **6.6 Backup, Regulatory Availability and Tier-IV Requirement**

Critical records must be backed up and protected against loss. The Company must confirm the arrangement ensuring that digital critical player, gaming and financial records are available to the CGA at all times on a server of a Tier-IV certified data centre registered in Curaçao.

The current reference to Curaçao VPS Hosting is not sufficient without evidence of data centre name, certification, registration, server location, scope of records, synchronisation frequency, backup, security controls and CGA availability mechanism.

### **6.7 Data Integrity, Corrections and Secure Destruction**

Corrections, adjustments or amendments to records must preserve the original record, amended record, reason, approver, timestamp, supporting evidence and audit trail. Manual adjustments to balances, payments, gaming results or compliance records require approval and audit logging.

Secure destruction after retention expiry must be documented and must not occur where a legal hold, complaint, AML / sanctions matter, regulatory request, dispute, investigation or litigation hold applies.

## Records and Evidence

| Record / evidence item                           | Status    |
|--------------------------------------------------|-----------|
| Player account records                           | Available |
| Gaming transaction records and export capability | Available |
| Financial transaction records and reconciliation | Available |
| AML/KYC records                                  | Available |
| Sanctions/TFS records                            | Available |
| Responsible gaming records                       | Available |
| Complaints/ADR records                           | Available |
| System logs and audit trails                     | Available |
| Retention schedule                               | Available |
| Tier-IV Curaçao data centre evidence             | Available |
| CGA availability mechanism                       | Available |

## 7. Player-Facing Website and Visual Elements

### 7.1 Principal Player-Facing Interface

The principal player-facing interface is Bahisbey.com and associated approved domain aliases. The Company shall maintain a register of all player-facing domains, aliases, redirects, mobile versions, mirror pages, landing pages and alternative interfaces.

The register must identify the purpose, status, licence display, Terms and Conditions link, Privacy Notice link, Responsible Gaming link, Complaints / ADR link, payment page, bonus pages and evidence screenshots for each interface.

### 7.2 Website Disclosure Principles

Player-facing disclosures must be accurate, current, clear and consistent with actual operations. The website must not misstate licence status, operator identity, approved domains, payment methods, crypto assets or networks, product availability, certification, payout speed or service availability.

All material disclosures must be reviewed when products, payment methods, crypto assets, Terms and Conditions, complaint routes, ADR provider, licence status or responsible gaming tools change.

### 7.3 Operator, Licence and Registration Interface

The website should identify the legal operator name, registration details, registered address, licence reference, regulator, verification or seal, contact details, responsible gaming link and complaints link.

The registration interface should collect required information for account creation, eligibility, KYC / AML, age verification, jurisdiction controls and Terms and Conditions acceptance. Acceptance evidence must be retained with version, date, time, IP/device data where available and account identifier.

#### 7.4 Account, Game and Payment Interface

The account area should show account details, balances, transaction history, KYC status, payment methods, responsible gaming tools, restrictions, communication preferences and policy links.

Game interfaces must provide accessible rules, settlement logic, limits, payout information, jackpot rules, bonus conditions, malfunction rules and complaint information. Payment pages must disclose methods, currencies, crypto assets / networks, limits, processing times, ownership requirements, KYC checks, third-party prohibition, unsupported network warnings, holds and fees.

#### 7.5 Responsible Gaming, Complaints and ADR Interface

The website shall make responsible gaming tools accessible, including deposit limits, loss limits, session limits, reality checks, cooling-off, self-exclusion, responsible gaming information and contact routes.

The complaints interface must explain complaint submission, required information, internal process, timeframes, escalation and ADR provider. Appointment of ADR is not sufficient unless EGIS-FZCO is disclosed in the Terms and Conditions and complaints interface.

#### 7.6 Terms and Conditions, Privacy and Promotions

Terms and Conditions must be accessible before registration, during account use and through the website. Acceptance must be recorded and historical versions archived. The Privacy Notice must explain data processing for registration, KYC, AML, sanctions, payments, gameplay, responsible gaming, complaints and security.

Bonus and promotion displays must disclose eligibility, wagering, expiry, limits, exclusions, restrictions and full terms without misleading players. Promotions must not target self-excluded or restricted players where suppression is required.

#### 7.7 Website Change Control and Screenshot Evidence

Material website changes to operator or licence information, Terms and Conditions, payments, crypto networks, responsible gaming tools, complaints / ADR, product rules, bonus terms, privacy, affiliate landing pages or UI elements affecting controls shall be reviewed before publication and archived.

Screenshots should be retained for homepage, licence display, registration, Terms and Conditions acceptance, account area, payments, crypto warnings, responsible gaming, complaints, ADR, Privacy Notice, game rules and promotions.

#### Records and Evidence

| Record / evidence item                       | Status    |
|----------------------------------------------|-----------|
| Domain / alias / redirect register           | Available |
| Homepage and licence screenshots             | Available |
| Registration and T&Cs acceptance screenshots | Available |
| Game/product screenshots                     | Available |

|                                              |           |
|----------------------------------------------|-----------|
| Payment and crypto warning screenshots       | Available |
| Responsible gaming page and tool screenshots | Available |
| Complaints page and ADR screenshots          | Available |
| Privacy Notice                               | Available |
| Website change-control records               | Available |

## 8. Access Controls and Excluded / Banned Persons

### 8.1 General Access Control Principles

The Company shall prevent use by underage persons, unregistered persons, ineligible persons, persons in prohibited jurisdictions, sanctioned persons, self-excluded persons, persons subject to cooling-off or other responsible gaming restrictions, banned persons, duplicate-account users, third-party payment users, persons using false information and any other prohibited persons.

Controls operate through registration, KYC, sanctions screening, jurisdiction controls, responsible gaming controls, payment checks, account monitoring, duplicate detection and manual Compliance review.

### 8.2 Age, Registration and KYC Controls

Registration must collect date of birth and eligibility confirmation, and age must be verified through KYC where required. Registration controls should include mandatory fields, Terms and Conditions acceptance, Privacy Notice acknowledgement, duplicate-account prohibition, false-information prohibition, jurisdiction restrictions, email or mobile verification and escalation of risk indicators.

Sumsub is identified as the KYC / AML provider, but the enabled modules, age-verification configuration, proof-of-address configuration, sanctions screening, PEP screening, adverse media screening and ongoing rescreening must be confirmed.

### 8.3 Prohibited or Restricted Jurisdictions

The Company shall maintain controls to restrict access from prohibited or restricted jurisdictions aligned with law, licence conditions, risk appetite, AML/CFT/CPF risk, sanctions, payment provider restrictions, supplier restrictions and Terms and Conditions.

Controls may include registration country, IP address, geolocation, payment country, KYC document country, phone country, device indicators and manual Compliance review. The prohibited or restricted jurisdiction list must be kept current and reflected in the Terms and Conditions and platform configuration.

### 8.4 Sanctions and TFS Controls

Sanctions screening shall apply at onboarding, KYC / CDD, ongoing monitoring, payment processing, withdrawal approval, crypto wallet review, account reactivation and material changes to player data.

Potential matches must restrict the account or transaction pending review. True matches must be escalated to the MLRO / Compliance Officer and frozen where required. Player communications must not disclose sensitive sanctions logic or authority reporting.

### 8.5 Self-Exclusion, Cooling-Off and Vulnerability

Self-excluded players must be prevented from deposits and gameplay, with marketing suppression and duplicate-account monitoring. Cooling-off shall temporarily restrict access according to the selected duration and platform configuration.

Vulnerable-player indicators such as distress, escalating deposits, repeated failed deposits, repeated withdrawal reversals, attempts to bypass restrictions or complaints alleging harm must be escalated to the responsible gaming owner and Compliance.

### 8.6 Duplicate Accounts, VPN and Banned Persons

Duplicate account indicators include same identity, device, IP, payment method, wallet, address, similar contact details, KYC failures, bonus abuse, self-exclusion circumvention or prohibited jurisdiction circumvention.

VPN, proxy, emulator or location-masking indicators must be reviewed where they indicate risk. Banned persons shall be blocked through account status, login restrictions, deposit and gameplay restrictions, payment method review and manual Compliance controls.

### 8.7 Account Suspension, Closure and Communications

Accounts may be suspended, blocked or closed for underage registration, failed KYC, prohibited jurisdiction, sanctions match, fraud, third-party payment, duplicate account, responsible gaming restrictions, AML concerns, breach of Terms and Conditions, regulatory instruction or other lawful grounds.

Player communications must be approved where sensitive and must not disclose AML, sanctions, fraud monitoring details, FIU reporting, authority correspondence or non-tipping-off information.

### Records and Evidence

| Record / evidence item                   | Status    |
|------------------------------------------|-----------|
| Age-verification process                 | Available |
| Registration flow screenshots            | Available |
| KYC / Sumsb configuration                | Available |
| Prohibited jurisdiction list             | Available |
| Sanctions workflow                       | Available |
| Self-exclusion/cooling-off configuration | Available |
| Duplicate-account controls               | Available |
| VPN / proxy detection                    | Available |
| Banned-person controls                   | Available |

|                                      |           |
|--------------------------------------|-----------|
| Customer Support escalation guidance | Available |
|--------------------------------------|-----------|

## 9. Responsible Gaming Implementation Interface

### 9.1 Purpose and Framework

This section describes how responsible gaming principles are operationally implemented through the platform. It does not replace the standalone Responsible Gaming Policy. The Company shall maintain a responsible gaming framework covering underage prevention, responsible gaming information, limits, reality checks, cooling-off, self-exclusion, marketing suppression, vulnerable-player indicators, customer communications, complaints, recordkeeping and training.

### 9.2 Governance and Tools

Based on available confirmations, Justice Nwankwo handles compliance, responsible gaming, complaints and related functions, subject to formal appointment evidence and scope confirmation. Current tools confirmed operationally include deposit limits, loss limits, session limits, reality checks, cooling-off, self-exclusion and marketing suppression upon activation, subject to configuration evidence.

The Company must confirm the responsible gaming owner, deputy, escalation route, reporting process, case register and supplier responsibility for implementation and evidence.

### 9.3 Deposit, Loss, Session Limits and Reality Checks

Deposit limits must define available periods, effective time, decrease and increase rules, pending deposits, payment interaction, staff override restrictions and retained records. Loss limits must define calculation method, period, products covered and effect once the limit is reached.

Session limits and reality checks must define notification frequency, acknowledgement requirements, products covered, effect of non-acknowledgement and recordkeeping. Configuration evidence and screenshots must be retained.

### 9.4 Cooling-Off and Self-Exclusion

Cooling-off must define available periods, activation, effect on deposits and gameplay, withdrawal handling, marketing suppression and reactivation. Self-exclusion must define available periods, immediate account effect, prevention of deposits and gameplay, withdrawal handling, marketing suppression, duplicate-account monitoring and reactivation rules.

The Company must test that self-exclusion and cooling-off restrictions operate as described and that marketing suppression is triggered automatically or through a documented manual process.

Where a player voluntarily requests self-exclusion due to problematic gambling behaviour, the Company shall apply an exclusion period of at least twelve months and shall treat the exclusion as irrevocable during that period, unless applicable law, licence conditions or an approved responsible gaming procedure requires a stricter outcome. The platform configuration, responsible gaming policy and Terms and Conditions must be aligned with this requirement and supported by testing evidence.

## 9.5 Marketing Suppression and Vulnerable-Player Indicators

Players under relevant responsible gaming restrictions must be excluded from email, SMS, push notifications, account messages, bonuses, retargeting where controlled and other promotional communications.

Vulnerable-player indicators include distress statements, repeated withdrawal reversals, failed deposits, escalating deposits, limit increase requests, attempts to bypass restrictions, duplicate-account activity and complaints alleging harm. Indicators must be escalated and documented.

## 9.6 AML / KYC / Payment Interaction

Responsible gaming information may overlap with AML / KYC and payment controls, including unusual deposit activity, repeated failed deposits, rapid spend increases, multiple payment methods, repeated withdrawal cancellation and financial pressure statements.

Responsible gaming intervention does not replace AML review, and AML review does not avoid player-protection action. Where both frameworks are relevant, Compliance must consider both.

## 9.7 Customer Support, Complaints and Supplier Interface

Customer Support must identify and escalate responsible gaming concerns and must not encourage gambling where distress is apparent, offer bonuses to reverse restrictions, remove restrictions without authorisation or send marketing to restricted players.

Where responsible gaming tools are implemented by Digitain, evidence of availability, configuration, restriction logic, marketing suppression, testing and reporting must be retained.

### Records and Evidence

| Record / evidence item                           | Status               |
|--------------------------------------------------|----------------------|
| Responsible Gaming Policy                        | Uploaded & Available |
| Responsible gaming owner appointment             | TBC                  |
| Deposit/loss/session/reality-check configuration | Available            |
| Cooling-off and self-exclusion configuration     | Available            |
| Responsible gaming screenshots                   | Available            |
| Marketing suppression workflow                   | Available            |
| Vulnerable-player trigger list                   | Available            |
| Responsible gaming case register and complaints  | Available            |
| Digitain responsible gaming evidence             | Available            |
| Responsible gaming training records              | Available            |

## **10. Terms and Conditions**

### **10.1 Current Terms and Conditions and Accessibility**

The Company shall maintain a current version of the Terms and Conditions. The current Terms and Conditions must be annexed to or stored with this Manual. A website link alone is not sufficient unless the full text, version number, effective date, publication URL, approval record, archive copy and player acceptance evidence are retained.

The Terms and Conditions must be accessible before registration, during account use and through the website, including from the homepage, registration interface, account area, payment pages, bonus pages and support or complaints pages where relevant.

### **10.2 Operator and Licence Disclosure**

The Terms and Conditions shall accurately identify the legal operator, registration details, registered address, licence reference, regulator, brand, domains, verification or seal, customer support and complaints contact details.

Licence reference OGL/2024/1601/0909 remains subject to confirmation against the current licence certificate and CGA records.

The Terms and Conditions must include a Curaçao governing law and jurisdiction clause consistent with applicable LOK requirements, including that the gaming agreement is subject to Curaçao law and that disputes relating to the gaming agreement may be brought before the competent Curaçao courts, without prejudice to the required complaint and ADR process.

### **10.3 Scope and Consistency**

The Terms and Conditions shall accurately reflect approved domains, product verticals, game and sportsbook rules, bet and payout limits, payment methods, crypto assets and networks, KYC, AML, sanctions, responsible gaming tools, complaints and ADR, bonus rules, privacy, account suspension and withdrawal controls.

They must not contradict actual supplier functionality, platform configuration, payment flows, internal procedures or regulator-facing documents.

### **10.4 Eligibility, KYC and AML Provisions**

The Terms and Conditions should state minimum age, accurate information requirement, prohibition on false, third-party and duplicate accounts, jurisdiction restrictions, account security duties and the Company's right to suspend, restrict or close accounts.

They should describe KYC, CDD, EDD, sanctions screening, payment ownership, crypto wallet ownership, source of funds and source of wealth requests, holds, reporting obligations and confidentiality restrictions.

### **10.5 Payment and Crypto Terms**

Payment provisions must describe deposit and withdrawal methods, currencies, limits, processing times, ownership, third-party prohibition, chargebacks, withdrawal verification, payment holds, refunds, balance rules and no credit.

Crypto terms must address supported assets and networks, unsupported network risk, wallet ownership, same-wallet controls, blockchain confirmations, monitoring, sanctions and wallet-risk screening, privacy

coins or mixers where prohibited, source-of-funds evidence, fees, volatility, conversion and mistaken deposits.

### 10.6 Funds, Winnings, Game Rules and Promotions

The Terms and Conditions should describe balances, winnings, withdrawals, delays, refusals, chargebacks, account closure balances, AML / sanctions / fraud / responsible gaming holds and the fact that the Company is not a financial institution.

They must include or link to sportsbook, casino, live casino, slots, virtual sports, jackpot and bingo rules; settlement; void and cancellation; malfunction; maximum payouts and complaint routes. Bonus terms must include eligibility, wagering, expiry, conversion, exclusions, abuse rules and responsible gaming restrictions.

### 10.7 Responsible Gaming, Complaints and ADR

The Terms and Conditions should address responsible gaming tools, limits, cooling-off, self-exclusion, marketing suppression and the Company's right to impose restrictions.

Complaints and ADR provisions must explain complaint channel, information required, process, timeframes, escalation, ADR provider, ADR availability to players where applicable and link to the Complaints Policy. EGIS-FZCO must be disclosed in the Terms and Conditions and complaints interface.

### 10.8 Amendments, Privacy and Approval

The Terms and Conditions shall link to the Privacy Notice and reflect actual data flows. Material amendments must be legally and operationally reviewed, archived and notified or accepted where required.

Review should involve Legal, MLRO / Compliance Officer, Payments, Product, Customer Support, Responsible Gaming, Information Security and senior management or the Board where material.

### Records and Evidence

| Record / evidence item                          | Status               |
|-------------------------------------------------|----------------------|
| Current Terms and Conditions                    | Uploaded & Available |
| Terms and Conditions version and effective date | Available            |
| Publication URL and archive                     | Available            |
| Acceptance records                              | Available            |
| Operator/licence disclosure                     | Available            |
| Payment clauses                                 | Available            |
| Crypto clauses                                  | Available            |
| Game/sportsbook rules                           | Available            |
| Responsible gaming clauses                      | Available            |

|                                                           |           |
|-----------------------------------------------------------|-----------|
| Complaints/ADR clauses                                    | Available |
| Privacy Notice link                                       | Available |
| Amendment workflow                                        | Available |
| Curaçao governing law and competent Curaçao courts clause | Available |

## 11. Player Complaints and Dispute Settlement

### 11.1 General Complaint Principles

The complaint process shall be fair, accessible, documented, timely and capable of regulatory review. Players must have a clear route to submit complaints; complaints must be recorded, objectively reviewed, supported by evidence, answered clearly and escalated where unresolved.

AML, sanctions, fraud, security and regulatory-sensitive information must not be disclosed inappropriately in complaint responses.

### 11.2 Complaint Policy and Channel

The Complaints Policy is the primary internal document for intake, registration, investigation, timeframes, escalation, ADR referral, recordkeeping, reporting and corrective actions.

The player-facing complaint channel should explain how to submit a complaint, information required, expected process, escalation route, ADR provider details and links to the Complaints Policy and Terms and Conditions.

The player-facing complaint process should state that complaints may be submitted free of charge and, where applicable, within six months after the relevant incident, settlement or disputed event. The complaint form or intake mechanism should request sufficient information to identify the player, account, disputed transaction or event, date, description, amount where relevant, supporting evidence and preferred contact language.

### 11.3 Complaint Intake and Register

Each complaint must be entered in the complaint register with reference, date, player ID, category, summary, product or transaction, amount, evidence, handler, escalation, response due date and outcome.

Complaint categories may include deposits, withdrawals, crypto, KYC, account suspension, game settlement, sportsbook, bonus, responsible gaming, self-exclusion, marketing after restriction, technical error, support conduct, fraud or privacy.

### 11.4 Investigation and Evidence

Complaint investigations should collect account records, KYC records, payment records, crypto transaction hashes, game or bet records, bonus records, responsible gaming records, support communications, logs, supplier evidence, relevant Terms and Conditions version and any prior player communications.

Supplier-related complaints require supplier evidence, including incident reports, game logs, settlement evidence, provider payment records or technical explanations.

## 11.5 Response, Timeframes and Compliance Escalation

Responses should acknowledge the complaint, summarise the issue, provide the outcome, explain the basis for the decision, identify corrective action where applicable and explain any further route including ADR where applicable.

Complaint timeframes must be aligned with the Company's Complaints Policy and applicable Curaçao requirements. As a minimum operational standard, the Company should provide acknowledgement within one week, issue a decision within four weeks where possible, and document any permitted written extension, escalation or ADR referral. Where the Company applies shorter internal targets, such as two business days for acknowledgement or five business days for responsible gaming complaints, those targets must be reflected consistently in the Complaints Policy, Terms and Conditions, customer support scripts and complaint register.

Complaints involving AML, sanctions, suspicious activity, payment ownership, crypto risk, fraud, underage gambling, responsible gaming, self-exclusion, account restrictions, regulatory threats or material supplier failure must be escalated to Compliance.

## 11.6 Responsible Gaming, Payment and Game Complaints

Responsible gaming complaints require review for system failure, staff failure, supplier failure, training gaps, corrective action and reporting. Payment complaints must be reviewed against provider records, KYC, AML, sanctions, ownership, responsible gaming restrictions and Terms and Conditions.

Game and sportsbook complaints require game round or bet ID, logs, supplier records, settlement source, rules, void or cancellation provisions, malfunction rules and payout rules.

## 11.7 ADR Provider and Escalation

The Company has confirmed EGIS-FZCO as ADR provider with accreditation reference CGA/ADR/2025/03, valid 9 February 2026 to 9 February 2029, contact [disputes@egis-adr.com](mailto:disputes@egis-adr.com), Dubai License No. 22105, Unit 22105-001, IFZA Business Park, DDP, Dubai, UAE.

The Company must retain appointment evidence, accreditation evidence, service terms, fee or cost arrangement, escalation procedure, records to be provided to ADR and player-facing disclosure in the Terms and Conditions and complaints interface.

The Company must ensure that ADR availability, ADR provider identity, contact route, timing, record production and cost treatment are clearly disclosed to players. ADR costs that must be borne by the licensee under applicable requirements must not be shifted to the player.

## 11.8 Reporting and Corrective Action

Complaint and ADR data should support internal reporting and regulatory reporting, including complaint numbers, categories, open and closed complaints, resolution times, ADR escalations, ADR outcomes, responsible gaming complaints, payment complaints, product complaints, recurring issues, supplier complaints and corrective actions.

Trends must be reviewed for control weaknesses and entered into the corrective action tracker where necessary.

## Records and Evidence

| Record / evidence item | Status |
|------------------------|--------|
|------------------------|--------|

|                                                   |                                |
|---------------------------------------------------|--------------------------------|
| Complaints Policy                                 | Uploaded & Available           |
| Complaint channel / page                          | Available                      |
| Complaint register                                | Available                      |
| Complaint timeframes                              | Available                      |
| Escalation matrix                                 | Available                      |
| EGIS-FZCO ADR appointment evidence                | Available                      |
| ADR disclosure in T&Cs                            | Uploaded & Available           |
| ADR disclosure on complaints page                 | Available as per the agreement |
| ADR service terms / fee arrangement               | Available as per the agreement |
| Complaint reporting template                      | Available                      |
| Complaint filing window, form and intake fields   | Available                      |
| Complaint acknowledgement and decision timeframes | Available                      |
| ADR cost treatment and player disclosure          | Available as per the agreement |

## 12. Technical Infrastructure and Business Continuity

### 12.1 Infrastructure Overview

Infrastructure includes player-facing domains, platform software, game and sportsbook systems, player account and wallet systems, payment and crypto integrations, KYC / AML, sanctions screening, responsible gaming tools, support tools, reporting and audit tools, databases, logs, hosting, backup, restoration and regulatory data availability.

Digitain supports platform, games and technical/security/incident functions, but Oxilium N.V. retains responsibility for the licensed operation, evidence availability and regulatory compliance.

### 12.2 Platform Provider

Digitain is identified as platform provider and game/sportsbook supplier. Evidence must confirm legal entity, agreement, scope, verticals, player wallet, reporting, responsible gaming tools, technical support, security responsibilities, incident notification, business continuity and regulatory cooperation.

The Company must retain a responsibility matrix distinguishing Digitain's technical role from Oxilium's retained regulatory responsibilities.

### 12.3 Hosting Environment and Tier-IV Requirement

Current hosting reference is Curaçao VPS Hosting - Ubuntu 18.04, 20 GB Disk, 5 Mbps connection, 1 Dedicated IP. This is not sufficient by itself to evidence compliance, resilience, security, record availability or Tier-IV status.

The Company must evidence data centre name, Tier-IV certification, Curaçao registration, server location, owner or contracting party, scope of records, synchronisation frequency, backup, encryption, access controls and CGA availability mechanism.

### 12.4 Technical Diagram and Data Flow Map

The Company shall maintain an infrastructure diagram covering domains, DNS or routing, platform, game servers, sportsbook, wallet, payment providers, payment agent, crypto provider, KYC / AML, responsible gaming tools, support systems, databases, logs, backups, regulatory data mirror/server, hosting, network boundaries, access points and data flows.

The data flow map must identify data categories, source systems, receiving systems, supplier, processing or storage jurisdiction, access rights, retention, backup, export, regulatory availability and security controls.

### 12.5 Security, Access and Monitoring

Security controls shall include role-based access, least privilege, MFA, password controls, privileged access approval, access reviews, encryption, logging, vulnerability and patch management, malware controls, firewalls, supplier access restrictions and incident response.

Access to player data, financial data, KYC / AML records, game configuration and platform configuration must be limited, approved and logged.

### 12.6 Backup, Restoration, Business Continuity and Disaster Recovery

Backup and restoration must cover player records, gaming records, financial records, KYC / AML records, sanctions records, responsible gaming records, complaint records, payment records, crypto records, logs, Terms and Conditions archives and regulatory reporting records.

The Information Security Policy references RTO up to 24 hours and RPO up to 4 hours; applicability must be evidenced. Business continuity and disaster recovery must cover outages, supplier failure, security incidents, data loss, regulatory-access failure and key person unavailability.

### 12.7 Incident Response and Change Management

Technical incidents, including platform, hosting, game, sportsbook, payment, crypto, KYC / AML, responsible gaming, data breach, unauthorised access, data corruption, backup or regulatory-access failures, must be logged, assessed, escalated and remediated.

Material changes to platform, products, suppliers, payment methods, crypto assets, KYC / AML, sanctions, hosting, reporting, responsible gaming tools and security configuration require testing, approval and documentation.

### Records and Evidence

| Record / evidence item           | Status    |
|----------------------------------|-----------|
| Technical infrastructure diagram | Available |

|                                                  |           |
|--------------------------------------------------|-----------|
| Data flow map                                    | Available |
| Digitain agreement / SLA / responsibility matrix | Available |
| Hosting agreement and technical specification    | Available |
| Tier-IV Curaçao data centre evidence             | Available |
| CGA regulatory data availability mechanism       | Available |
| Access-control matrix                            | Available |
| Backup schedule and restoration tests            | Available |
| Business continuity / disaster recovery plan     | Available |
| Incident response procedure                      | Available |
| Monitoring/logging and change management         | Available |

### 13. AML/CFT/CPF Operational Interface

#### 13.1 Purpose

This section describes the operational interface between the Company's AML/CFT/CPF framework and the Bahisbey operation. It does not replace the standalone AML/CFT/CPF Policy and KYC Policy, which remain the primary policy documents for customer due diligence, risk assessment, monitoring, escalation, reporting, recordkeeping and governance.

#### 13.2 Policies and MLRO Responsibility

The AML/CFT/CPF Policy and KYC Policy govern CDD, EDD, customer risk assessment, sanctions, PEP, adverse media, transaction monitoring, unusual and suspicious transaction escalation, FIU / goAML reporting, recordkeeping, training, independent review and MLRO responsibilities.

Justice Nwankwo is identified as Compliance Officer / MLRO, subject to formal appointment evidence and scope confirmation. The MLRO / Compliance Officer is responsible for oversight of AML/CFT/CPF controls, escalation, reporting and evidence.

#### 13.3 Risk-Based Approach and Customer Due Diligence

The Company shall apply a risk-based approach considering player profile, jurisdiction, product, payment method, crypto wallet, transaction behaviour, source of funds, source of wealth, PEP status, adverse media, sanctions and responsible gaming indicators overlapping with financial risk.

CDD includes identity verification, age verification, address verification where required, sanctions screening, PEP screening, adverse media screening, customer risk assessment, payment ownership, wallet ownership and source of funds where required. Sumsb modules and configuration must be confirmed.

### **13.4 Enhanced Due Diligence**

EDD may apply to high-risk players, PEPs, adverse media matches, high-risk jurisdictions, inconsistent payment activity, crypto wallet-risk, unclear source of funds or source of wealth, third-party payment concerns, unusual or suspicious indicators, high-value or rapid transactions and responsible gaming indicators overlapping with financial-risk concerns.

EDD decisions must be approved, documented and linked to player activity, payment activity, source-of-funds evidence, wallet evidence and monitoring outcomes.

### **13.5 Sanctions Interface and Transaction Monitoring**

Sanctions controls operate at onboarding, ongoing monitoring, payments, withdrawals, crypto wallet review and supplier due diligence. Potential matches must be restricted and escalated pending review.

Transaction monitoring covers deposits, withdrawals, rapid deposit-withdrawal activity, minimal gameplay, high-value transactions, structuring, multiple payment methods, third-party indicators, ownership inconsistencies, wallet-risk, unsupported networks, bonus abuse and behaviour inconsistent with player profile.

### **13.6 Crypto AML Controls**

Crypto AML controls should include supported asset and network controls, wallet ownership, transaction hash retention, wallet-risk screening, sanctions screening, source-of-funds review, same-wallet or equivalent withdrawal control, unsupported asset or network handling, review of mixers, tumblers, darknet exposure, scams, hacks and high-risk services, escalation and documentation.

The Cryptocurrency Risk Management Policy must reflect USDT TRC, USDT ERC and USDC ERC if those assets and networks are active.

### **13.7 Payment Ownership and Suspicious Activity Escalation**

Attempted or suspected third-party payments are AML risk indicators requiring Compliance review. The Company may request evidence, reject payment methods, suspend withdrawals, restrict accounts, refund funds where lawful, conduct EDD, consider reporting or close accounts.

Unusual or suspicious matters may be triggered by monitoring alerts, KYC / EDD, sanctions, payment ownership, crypto alerts, responsible gaming or financial distress indicators, support observations, supplier alerts or authority requests.

### **13.8 FIU / goAML, Non-Tipping-Off and Records**

Where reporting is required, the Company must maintain goAML registration, authorised users, reporting workflow, approvals, submission records, supporting evidence, FIU correspondence and confidentiality controls.

Personnel must not disclose suspicious activity reports, monitoring rules, sanctions logic, FIU correspondence or investigations to players or unauthorised parties. AML records must be secure, access-controlled and retrievable.

### **13.9 Training, Independent Review and Supplier Interface**

AML/CFT/CPF training must cover gaming risks, CDD / EDD, sanctions, transaction red flags, crypto risk, payment ownership, suspicious escalation, goAML, non-tipping-off, recordkeeping and customer communication limitations.

Independent review or audit should assess governance, MLRO independence, CDD / EDD, sanctions, transaction monitoring, crypto controls, reporting, records, training and suppliers. Supplier evidence is required for Sumsb, payment providers, Spinmatic, CoinPayments, Digitain and hosting.

## Records and Evidence

| Record / evidence item                       | Status               |
|----------------------------------------------|----------------------|
| AML/CFT/CPF Policy                           | Uploaded & Available |
| KYC Policy                                   | Uploaded & Available |
| MLRO appointment                             | Appointed            |
| Customer risk assessment methodology         | Available            |
| Sumsb agreement/configuration                | Available            |
| Sanctions configuration                      | Available            |
| Transaction monitoring rules                 | Available            |
| Crypto AML controls                          | Available            |
| Internal suspicious activity report template | Available            |
| goAML registration and FIU workflow          | Available            |
| AML training records                         | Available            |
| Independent AML review                       | Available            |

## 14. Sanctions and Targeted Financial Sanctions

### 14.1 Purpose of this Section

This section describes the Company's operational framework for sanctions and targeted financial sanctions controls applicable to Bahisbey.com and associated approved domain aliases. It documents how the Company identifies, screens, escalates, freezes, records and reports sanctions-related matters involving players, payment activity, crypto transactions, suppliers, counterparties and other relevant persons.

### 14.2 General Sanctions Principles

The Company shall not knowingly provide services to persons, entities, wallets, payment instruments, suppliers or counterparties subject to applicable sanctions or targeted financial sanctions.

The Company shall maintain controls designed to screen players at onboarding, conduct ongoing rescreening, screen relevant payment activity, screen crypto wallet exposure where applicable, review suppliers and counterparties, identify potential matches, escalate possible matches to the MLRO / Compliance Officer, freeze or restrict assets where legally required, prevent prohibited transactions, report to competent authorities where required and retain records.

Sanctions controls must operate independently of commercial considerations. A transaction, player or supplier must not be permitted to proceed where a true sanctions match or freezing obligation applies.

### **14.3 Governance and Responsibility**

The MLRO / Compliance Officer is responsible for sanctions and targeted financial sanctions oversight, including maintaining sanctions screening controls, ensuring screening applies at relevant stages, reviewing potential matches, determining whether escalation is required, coordinating freezing actions, coordinating reporting, maintaining records, ensuring training and escalating material sanctions issues to senior management or the Board.

Operational teams, Customer Support, Payments and suppliers shall escalate sanctions alerts to the MLRO / Compliance Officer and shall not independently clear potential matches unless authorised under an approved procedure.

### **14.4 Screening Scope**

The Company shall apply sanctions screening to relevant persons, entities and transactions, including players, beneficial owners or linked persons where identified, payment method owners, crypto wallets, suppliers, payment agents, payment providers, crypto providers, affiliates or referral partners, ADR provider, key employees or officers where relevant and other counterparties requiring sanctions due diligence.

Screening shall be performed using approved screening tools, supplier systems or documented manual controls.

### **14.5 Screening Points**

Sanctions screening shall be conducted at appropriate points in the player lifecycle and operational process, including registration, KYC / identity verification, before first withdrawal, when player details change, periodic or ongoing rescreening, list updates, before releasing held funds, account reactivation, high-risk transactions, crypto withdrawals, payment ownership concerns and authority or supplier alerts.

As a minimum control, sanctions status should be checked or reconfirmed before withdrawals are released, particularly where the player has not recently been screened, where player details have changed, where a high-risk payment method or crypto wallet is involved, or where a sanctions list update has occurred.

### **14.6 Screening Lists and Data Sources**

The Company shall ensure that sanctions screening is conducted against relevant sanctions and targeted financial sanctions lists. The screening configuration should identify list sources used, whether relevant Curaçao, Dutch Kingdom, EU, UN, OFAC, UK and other lists are covered where applicable, update frequency, matching logic, transliteration and alias handling, date-of-birth and nationality matching, false-positive handling, rescreening mechanism and audit trail.

The Company must confirm the actual list coverage and configuration used by Sumsb or any other screening provider.

### **14.7 Potential Match Review**

Where a potential sanctions match is identified, the Company shall restrict the relevant account, transaction or relationship pending review. The review shall include player or counterparty identity data, screening result, list source, matching fields, supporting documents, payment or wallet information,

transaction activity, false-positive analysis, reviewer name, date and time of review, decision and escalation outcome.

Potential match decisions shall be documented and retained. Customer Support must not inform the player that a sanctions match or sanctions investigation is being reviewed unless communication has been approved by the MLRO / Compliance Officer and is legally appropriate.

#### **14.8 False Positives**

Where a potential match is determined to be a false positive, the Company shall document the basis for clearance, including screening result, identity information compared, mismatch factors, supporting documents reviewed, reviewer, approval, date and time and any conditions or monitoring applied.

Repeated false positives should be monitored to determine whether screening configuration or customer data quality requires improvement.

#### **14.9 True Matches and Freezing**

Where a true sanctions match or freezing obligation is identified, the Company shall immediately restrict the account, transaction, payment method, wallet or relationship as required. The Company shall stop further transactions, freeze funds or economic resources where required, prevent deposits, withdrawals and gameplay as required, preserve records, escalate immediately to the MLRO / Compliance Officer, report to competent authorities where required, maintain confidentiality and document all actions.

Where targeted financial sanctions or asset-freezing obligations apply, the Company shall freeze funds or economic resources without delay and without prior notice to the player or counterparty, restrict further activity, preserve records and escalate immediately to the MLRO / Compliance Officer. No withdrawal, refund, transfer, conversion or release may occur unless legally permitted and appropriately authorised.

Frozen funds must not be released, refunded, transferred, converted or otherwise dealt with unless legally permitted and appropriately approved.

#### **14.10 Frozen Asset Register and Reporting**

The Company shall maintain a frozen asset register including player or counterparty name, account identifier, screening result, list source, freeze date and time, assets or funds frozen, currency or crypto asset, balance at freeze time, transactions stopped, authority notified, report reference, review status, unfreezing approval where applicable and final outcome.

Where sanctions laws or targeted financial sanctions obligations require reporting to a competent authority, the Company shall submit the required report within the applicable timeframe and through the applicable channel.

#### **14.11 Crypto Wallet Sanctions and Blockchain-Risk Controls**

Where crypto payments are accepted, the Company shall apply sanctions and wallet-risk controls to relevant wallet activity. Controls should include wallet ownership verification, wallet-risk screening, sanctions exposure review, review of exposure to sanctioned addresses, mixers, tumblers, darknet markets, hacks, scams or high-risk services, transaction hash retention, blockchain confirmation review, escalation of high-risk wallet activity and restriction of transactions pending review.

The Company shall confirm whether CoinPayments / UAB Star Ventures, Sumsub or another provider performs wallet-risk screening and what screening evidence is available to Oxilium N.V.

### 14.12 Supplier and Counterparty Sanctions Due Diligence

The Company shall perform sanctions due diligence on relevant suppliers and counterparties, including platform provider, game suppliers, payment providers, payment agent, crypto payment provider, KYC / AML provider, hosting provider, ADR provider, affiliates, referral partners and material outsourced service providers. Supplier sanctions checks should be performed before onboarding and periodically thereafter for material suppliers.

### 14.13 Player Communications, Records, Training and Testing

Communications with players regarding sanctions-related restrictions shall be carefully controlled. The Company shall not disclose screening logic, list-matching details, internal investigation steps, reporting decisions, FIU or authority correspondence, freezing decision details beyond what is legally appropriate or any information that may breach confidentiality or non-tipping-off obligations.

Records shall include screening results, potential match reviews, false-positive clearances, true-match decisions, freezing records, frozen asset register, authority reports, authority correspondence, player communications, supplier screening records, crypto wallet screening records and training records. Periodic review should test screening configuration, list coverage, update frequency, rescreening, false positives, freezing workflow, frozen asset register, crypto wallet screening, supplier screening, reporting route and staff training.

#### Records and Evidence

| Record / evidence item                | Status    |
|---------------------------------------|-----------|
| Sanctions / TFS procedure             | Available |
| Sanctions screening provider evidence | Available |
| List coverage and update frequency    | Available |
| Potential match workflow              | Available |
| False-positive clearance records      | Available |
| True-match escalation workflow        | Available |
| Freezing process                      | Available |
| Frozen asset register                 | Available |
| Competent authority reporting route   | Available |
| Crypto wallet screening evidence      | Available |
| Supplier sanctions checks             | Available |
| Player communication templates        | Available |
| Sanctions training records            | Available |

|                                                         |           |
|---------------------------------------------------------|-----------|
| Sanctions control testing evidence                      | Available |
| Freeze without delay and without prior notice procedure | Available |
| Withdrawal sanctions status check                       | Available |
| Freeze without delay / no prior notice workflow         | Available |
| Pre-withdrawal sanctions screening control              | Available |

## 15. Supplier and Outsourcing Management

### 15.1 Purpose and General Outsourcing Principles

This section describes the Company's supplier and outsourcing management framework for Bahisbey.com and associated approved domain aliases. It applies to platform, games, sportsbook, payments, crypto payments, KYC / AML, hosting, ADR, customer support, affiliates and other material operational functions.

The use of suppliers does not transfer regulatory responsibility away from Oxilium N.V. Supplier arrangements must be documented, monitored and capable of producing evidence for internal review, audit and regulatory inspection.

### 15.2 Supplier Register

The Company shall maintain a supplier register identifying supplier legal name, trading name, jurisdiction, registration number where available, service provided, regulatory status where applicable, contractual relationship, contract date, service start date, criticality rating, data processed, systems accessed, subcontractors where known, responsible internal owner, SLA or performance obligations, incident escalation contact, termination or exit arrangement and current status.

### 15.3 Current Supplier Overview

Based on operational confirmations currently available, Digitain supports platform, games and sportsbook; Bank Havale / bank transfers and Papara support fiat payments; Spinmatic Limited is payment agent; CoinPayments / UAB Star Ventures supports crypto; Sumsb supports KYC / AML; Curaçao VPS Hosting is referenced but role and sufficiency require confirmation; EGIS-FZCO is ADR provider; customer support is internally managed; and referral sites may be used for traffic.

This overview must be reconciled against contracts, invoices, technical evidence, service descriptions and operational records.

### 15.4 Supplier Due Diligence and Classification

The Company shall perform due diligence before onboarding material suppliers and periodically thereafter. Due diligence should include legal identity verification, corporate registration evidence, ownership and control review, sanctions screening, regulatory status review, licence or certification evidence, service capability assessment, information security assessment, data protection assessment,

AML/CFT/CPF relevance assessment, business continuity assessment, subcontractor review, reputation and adverse media review and conflict or dependency assessment.

Suppliers shall be classified according to risk and operational criticality. Critical suppliers should be subject to enhanced due diligence, written agreements, SLA review, incident escalation arrangements and periodic monitoring.

### **15.5 Written Agreements and Responsibility Matrix**

The Company shall maintain written agreements with material suppliers. Agreements should address scope, service levels, regulatory cooperation, audit and information rights, data protection, confidentiality, security controls, business continuity, incident notification, subcontracting restrictions, reporting, record retention, termination rights, exit assistance, governing law and dispute resolution.

The Company shall maintain a responsibility matrix identifying function performed by the supplier, function retained by the Company, approvals, escalation triggers, record owner, regulatory reporting responsibility, player communication responsibility, incident response responsibility, data export responsibility, audit and evidence provision and backup or contingency responsibility.

### **15.6 Digitain**

Digitain is currently identified as platform provider and provider of games and sportsbook functionality. The Company shall maintain written evidence confirming Digitain legal entity, agreement, platform scope, product verticals supported, sportsbook services, game supply or aggregation, wallet and player account functionality, responsible gaming tools, reporting and audit tools, technical support, security responsibilities, incident escalation, certification evidence, testing evidence, business continuity and regulatory cooperation obligations.

### **15.7 Sumsb**

Sumsb is currently identified as the KYC / AML provider. The Company shall maintain evidence confirming legal contracting entity, agreement, services provided, identity verification modules, proof of address functionality, age verification, sanctions screening, PEP screening, adverse media screening, ongoing rescreening, transaction monitoring or case-management functionality if applicable, data retention, access and reporting capability, escalation workflow and security and data protection obligations.

### **15.8 Payment, Crypto and Hosting Suppliers**

The Company shall maintain documentation for fiat payment providers and payment agent arrangements, including Papara, Bank Havale / bank transfers and Spinmatic Limited. Documentation must cover payment flows, settlement, reconciliation, ownership checks, AML / sanctions cooperation, chargebacks, incidents and termination.

The Company shall maintain documentation for CoinPayments / UAB Star Ventures and any crypto provider, including provider legal identity, agreement, regulatory status where applicable, supported assets, supported networks, wallet custody model, wallet ownership controls, transaction monitoring, wallet-risk screening, sanctions screening, reporting access, incident escalation and continuity.

The Company must clarify and document the exact role of the hosting provider currently described as Curaçao VPS Hosting and obtain hosting agreement, data centre evidence, Tier-IV certification and CGA availability mechanism.

## 15.9 ADR, Affiliates, Monitoring and Exit

The Company has confirmed EGIS-FZCO as ADR provider. Appointment of an ADR provider is not sufficient by itself; the Company must ensure that EGIS-FZCO is disclosed to players in the Terms and Conditions and complaints interface.

Affiliate and referral controls should include registers, due diligence, sanctions screening, agreements, traffic source identification, marketing restrictions, prohibited content restrictions, responsible gaming requirements, underage or misleading marketing prohibition, prohibited jurisdiction restrictions, monitoring, incident escalation and termination rights.

Supplier performance monitoring shall include SLA performance, availability, incidents, complaint trends, payment failure rates, KYC / screening failure rates, technical support response, security incidents, evidence provision and corrective actions. Exit planning should address termination, data transfer, continuity of records, alternative suppliers, regulatory notification and player communication where required.

### Records and Evidence

| Record / evidence item                        | Status    |
|-----------------------------------------------|-----------|
| Supplier register                             | Available |
| Supplier due diligence files                  | Available |
| Supplier criticality classification           | Available |
| Written supplier agreements                   | Available |
| Supplier responsibility matrix                | Available |
| Digitain agreement / SLA / technical evidence | Available |
| Digitain certification / testing evidence     | Available |
| Sumsu agreement and configuration             | Available |
| Payment provider documentation                | Available |
| Spinmatic Limited agreement                   | Available |
| CoinPayments / UAB Star Ventures agreement    | Available |
| Hosting agreement and data centre evidence    | Available |
| Tier-IV Curaçao data centre evidence          | Available |
| EGIS-FZCO ADR agreement / terms               | Available |
| ADR disclosure evidence                       | Available |
| Affiliate / referral register                 | Available |

|                             |           |
|-----------------------------|-----------|
| Supplier monitoring records | Available |
| Supplier incident records   | Available |
| Supplier exit plans         | Available |

## **16. Reports, Incidents and Regulatory Availability**

### **16.1 Purpose and Reporting Principles**

This section describes the Company’s framework for regulatory reporting, incident recording, escalation, regulatory availability of records and responses to requests from competent authorities in connection with Bahisbey.com and associated approved domain aliases.

The Company shall maintain procedures to identify and manage matters requiring regulatory notification, reporting, escalation or evidence production. Reports must be accurate, evidence-based, approved by the appropriate function and retained.

### **16.2 Regulatory Responsibility and Manual Availability**

The Board and senior management retain ultimate responsibility for ensuring that the Company complies with its reporting and regulatory availability obligations. The MLRO / Compliance Officer shall coordinate regulatory reporting and request-handling for compliance-sensitive matters.

This Manual must be complete, current, version-controlled, dated, approved, supported by evidence, reviewed periodically, updated following material changes, stored securely and available for inspection within the applicable regulatory timeframe.

The Company shall be able to produce the current Operations Manual and supporting records for CGA inspection within five working days after a CGA request, or within any shorter timeframe specified by law, licence condition or regulator instruction. The evidence repository and regulatory request log must support timely production.

### **16.3 Amendment Reporting**

The Company shall maintain records of amendments to this Manual and shall report amendments where required. Amendments may be required following licence status changes, approved domain changes, new products, payment methods, crypto assets or networks, supplier changes, hosting changes, responsible gaming changes, Terms and Conditions amendments, ADR changes, AML / KYC changes, sanctions changes, incidents or regulatory instruction.

The regulatory reporting calendar must include periodic amendment reporting where required, including twice-yearly amendment reporting deadlines of 15 June and 15 January where applicable. The Company must confirm the current CGA portal format, report owner, approval workflow and evidence package for such submissions.

### **16.4 Incident Reporting Framework and Register**

The Company shall maintain an incident reporting framework. Incidents may include platform outage, gaming system malfunction, sportsbook settlement failure, jackpot or bingo issue, payment provider failure, crypto payment incident, KYC / AML outage, sanctions screening failure, responsible gaming tool

failure, self-exclusion failure, complaint handling failure, data breach, unauthorised access, hosting failure, regulatory data availability failure, supplier incident, suspected fraud or criminal activity and any event affecting reliable, responsible, secure or compliant operation.

Incident reporting must include, where applicable, security breaches, equipment or software failures, player fraud or criminal behaviour and any other serious threat to responsible, reliable and verifiable gaming operations. Each incident must be assessed for CGA notification, player impact, corrective action and supplier involvement.

The incident register shall record incident reference, timing, category, systems or products affected, players affected, financial impact, regulatory impact assessment, owner, supplier involved, immediate actions, root cause, corrective action, regulatory reporting decision, date reported where applicable, closure date and post-incident review outcome.

### **16.5 Incident Classification and Types**

Incidents shall be classified by severity, impact and regulatory relevance. Classification factors include player impact, financial impact, number of players affected, duration, product or system affected, impact on responsible gaming, AML / KYC, sanctions, payments, gaming fairness, data security, regulatory record availability, supplier involvement and likelihood of recurrence.

Technical, game integrity, responsible gaming, AML/CFT/CPF, sanctions, payment, crypto and supplier incidents must be escalated to the relevant owner and assessed for regulatory reporting and corrective action.

### **16.6 Complaints, ADR and Regulatory Requests**

The Company shall maintain complaint and ADR records capable of supporting reporting and trend analysis, including complaint numbers, categories, open and closed complaints, average resolution time, ADR escalations, ADR outcomes, responsible gaming complaints, payment complaints, product complaints, recurring issues, supplier-related complaints and corrective actions.

The complaint and ADR reporting process must be aligned with the applicable CGA reporting framework, including any complaint reporting deadlines, report categories, required data fields and portal submission requirements. Where the Company reports complaints on 15 January and 15 June, the reporting calendar, complaint register and evidence repository must support those submissions.

Regulatory requests shall be logged, assigned and tracked. Requests may relate to the Manual, licence status, player records, gaming transaction records, financial transaction records, AML / KYC records, sanctions records, complaints, responsible gaming, incidents, suppliers, technical infrastructure, Terms and Conditions or training records.

### **16.7 Regulatory Data Availability**

The Company shall ensure that critical player, gaming and financial records are available for regulatory inspection in accordance with applicable requirements.

The Company must confirm the technical arrangement used to ensure that digital critical player, gaming and financial records are available to the CGA at all times on a server of a Tier-IV certified data centre registered in Curaçao. The current hosting information is not sufficient by itself to evidence this arrangement.

## **16.8 Evidence Production, Communications and Corrective Actions**

Where records are produced for regulatory inspection, audit, ADR or internal review, the Company shall maintain a production record identifying request reference, requester, records requested, records produced, production date, approver, confidentiality or privilege assessment, redactions if any and storage location. Regulatory communications must be accurate, complete, evidence-based, internally reviewed, consistent with Company records, retained and escalated where material. Corrective actions from incidents, reports, complaints, audits or requests must be recorded, assigned, monitored and closed with evidence.

## **17. Training and Awareness**

### **17.1 Purpose and General Training Principles**

This section describes the Company's training and awareness framework for personnel, officers, managers, customer support staff, compliance staff and other relevant persons involved in the operation of Bahisbey.com and associated approved domain aliases.

Training shall be role-specific, risk-based, documented, repeated periodically, updated following material regulatory, operational or policy changes, supported by attendance records, capable of audit or regulatory review and linked to the Company's policies, procedures and operational controls. Training is not complete unless attendance, materials, date, trainer and scope are recorded.

### **17.2 Training Governance**

The MLRO / Compliance Officer shall coordinate or oversee compliance-related training. Senior management shall ensure that relevant personnel receive adequate training and that training gaps are remediated.

Training ownership should be allocated for AML/CFT/CPF, sanctions and targeted financial sanctions, responsible gaming, complaints and ADR, customer communication standards, information security, data protection and confidentiality, anti-bribery and corruption, crime prevention, incident escalation, regulatory reporting and recordkeeping.

### **17.3 Mandatory Training Topics**

The Company shall ensure that relevant personnel receive training on AML/CFT/CPF, KYC / CDD / EDD, sanctions and targeted financial sanctions, unusual and suspicious transaction escalation, crypto payment risks, payment ownership and third-party payment risks, responsible gaming, underage gambling prevention, self-exclusion and cooling-off, complaints and ADR, customer communication standards, information security, data protection and confidentiality, anti-bribery and corruption, crime prevention, incident identification and escalation, supplier escalation, regulatory request handling and recordkeeping.

The annual training programme shall include, as applicable to the person's role, mental well-being and player protection, anti-bribery and corruption, crime prevention, responsible gaming, AML/CFT/CPF, sanctions and targeted financial sanctions, communication with players, complaints handling, responsible advertising and recordkeeping. Training content and attendance must be documented and retained.

### **17.4 AML/CFT/CPF and Sanctions Training**

AML/CFT/CPF training shall cover money laundering, terrorist financing and proliferation financing risks in remote gaming, CDD, EDD, customer risk assessment, transaction monitoring, red flags, internal

escalation, FIU / goAML reporting awareness, non-tipping-off, payment ownership controls, crypto payment red flags, recordkeeping and customer communication limitations.

Sanctions training shall cover screening points, potential match escalation, false-positive handling, true-match escalation, freezing obligations, frozen asset register, authority reporting, crypto wallet-risk exposure, supplier sanctions risk, confidentiality and approved player communication.

### **17.5 Responsible Gaming and Complaints Training**

Responsible gaming training shall cover responsible gaming principles, underage prevention, deposit limits, loss limits, session limits, reality checks, cooling-off, self-exclusion, marketing suppression, vulnerable-player indicators, player distress communications, escalation, complaints and interaction between responsible gaming, payments and AML/CFT/CPF.

Complaints and ADR training shall cover identifying complaints, recording complaints, complaint categories, complaint timeframes, evidence collection, escalation to Compliance, responsible gaming complaints, payment and withdrawal complaints, game settlement complaints, response standards, ADR escalation, EGIS-FZCO disclosure, confidentiality and communication limitations.

### **17.6 Information Security, Anti-Bribery and Customer Communication Training**

Information security and data protection training shall cover secure handling of player data, access-control responsibilities, password and MFA requirements, phishing, confidentiality of KYC / AML / sanctions / complaints records, secure handling of payment and crypto records, incident escalation, supplier access restrictions and secure communication.

Anti-bribery and crime prevention training shall cover prohibition on bribery and improper payments, gifts and hospitality, conflicts of interest, supplier and affiliate integrity, facilitation payment prohibition, suspicious external approaches, fraud indicators, manipulation or collusion concerns and employee misconduct.

Customer Support and other player-facing personnel shall be trained on professional communication, complaints, payment holds, KYC requests, responsible gaming concerns, avoiding misleading statements, avoiding disclosure of AML / sanctions monitoring logic, non-tipping-off, escalation and documentation.

### **17.7 Incident Escalation, Frequency and Records**

Relevant personnel shall receive training on identifying and escalating technical incidents, game integrity incidents, payment incidents, crypto incidents, KYC / AML incidents, sanctions incidents, responsible gaming incidents, complaints incidents, information security incidents, supplier incidents and regulatory data availability failures.

Training should occur before or shortly after onboarding into a relevant role, at least annually for core compliance topics, following material regulatory or policy changes, following material operational changes, after relevant incidents or control failures, after audit findings identifying training gaps and when a person changes role.

The training register shall record employee or participant name, role, department or function, training topic, training date, trainer or provider, delivery method, materials used, completion status, assessment result where applicable, refresher due date and evidence location.

## 17.8 Training Effectiveness and Supplier Personnel

The Company shall periodically assess training effectiveness through completion tracking, knowledge checks, case studies, quality assurance review, complaint review, incident review, audit findings, sample testing of staff responses and manager feedback.

Where supplier personnel perform or support regulated functions, the Company shall confirm whether they receive appropriate training or are subject to equivalent contractual obligations. This may apply to platform support, payment support, KYC / AML support, technical incident support, customer support if outsourced, responsible gaming tool support and complaint or ADR support.

### Records and Evidence

| Record / evidence item                                     | Status    |
|------------------------------------------------------------|-----------|
| Training policy or procedure                               | Available |
| Training calendar                                          | Available |
| Training owner / governance record                         | Available |
| AML/CFT/CPF training materials                             | Available |
| Sanctions / TFS training materials                         | Available |
| Responsible gaming training materials                      | Available |
| Complaints and ADR training materials                      | Available |
| Information security training materials                    | Available |
| Anti-bribery / crime prevention training materials         | Available |
| Customer communication training materials                  | Available |
| Incident escalation training materials                     | Available |
| Training attendance records                                | Available |
| Training register                                          | Available |
| Training effectiveness records                             | Available |
| Supplier training evidence                                 | Available |
| Annual training programme covering LOK/CGA required topics | Scheduled |

## **18. Registers and Evidence Schedule**

### **18.1 Purpose and General Evidence Principles**

This section identifies the registers, evidence files, logs and supporting records that the Company shall maintain in connection with Bahisbey.com and associated approved domain aliases. It creates a central evidence schedule supporting this Operations Manual, internal compliance review, audit readiness, regulatory inspection, complaint handling, ADR, incident review and Board oversight.

Evidence should be clearly named, version-controlled where applicable, dated, approved where required, linked to the relevant policy or procedure, stored securely, assigned to an owner, reviewed periodically and retained for the required period. Unverified screenshots, informal messages, verbal confirmations or unsupported supplier statements should not be treated as sufficient evidence for regulatory purposes unless supported by formal records.

### **18.2 Core Registers**

The Company shall maintain core registers including Operations Manual version log, Implementation Action Tracker, product register, game certification register, payment-method register, supplier register, complaint register, incident register, training register, sanctions / frozen asset register, regulatory request log and corrective action tracker.

Each register must identify owner, location, update frequency, access permissions, status and evidence source.

### **18.3 Corporate, Licence, Product and Game Evidence**

Corporate and licence evidence shall include certificate of incorporation, company extract, articles, ownership records, board and management appointments, current licence certificate, licence conditions, CGA portal status, approved domains, licence seal or verification evidence and Board approval of this Manual.

Product and game evidence shall include product register, full active game list, sportsbook rulebook and settlement evidence, casino, slots and live casino rules, virtual sports rules and mechanism, jackpot rules, bingo rules, RNG certificates, game certificates, RTP / PAR sheets where applicable and product change register.

### **18.4 Payment, Crypto, AML, KYC and Sanctions Evidence**

Payment and crypto evidence shall include payment-method register, Bank Havale / bank transfer documentation, Papara documentation, Spinmatic Limited agreement and matrix, CoinPayments / UAB Star Ventures agreement, supported crypto asset and network list, updated Cryptocurrency Risk Management Policy, deposit and withdrawal flows, payment and wallet ownership procedures, reconciliation records and confirmation that no player credit is offered.

AML/CFT/CPF and KYC evidence shall include AML/CFT/CPF Policy, KYC Policy, policy approvals, MLRO appointment, customer risk assessment methodology, Sumsud agreement and configuration, screening configuration, CDD and EDD records, transaction monitoring rules, goAML registration and FIU workflow, independent review evidence.

Sanctions evidence shall include sanctions / TFS procedure, screening provider evidence, list coverage, update frequency, match workflows, freezing process, frozen asset register, authority reporting route, crypto wallet screening evidence, supplier sanctions screening and sanctions training / testing.

## **18.5 Responsible Gaming, Complaints and ADR Evidence**

Responsible gaming evidence shall include Responsible Gaming Policy, policy approval, responsible gaming owner appointment, tool configurations, marketing suppression workflow, screenshots and testing evidence, vulnerable-player triggers, responsible gaming case records, complaint records and training evidence.

Complaints and ADR evidence shall include Complaints Policy, complaint channel, complaint register, complaint categories, response templates, escalation matrix, complaint timeframes, EGIS-FZCO appointment evidence, accreditation reference, validity period, ADR disclosure in Terms and Conditions and complaints page, ADR service terms and fee arrangement.

## **18.6 Technical Infrastructure, Website, Supplier and Training Evidence**

Technical infrastructure evidence shall include infrastructure diagram, data flow map, Digitain technical description, SLA and matrix, hosting agreement and role, Tier-IV Curaçao data centre evidence, CGA data availability mechanism, security controls, access-control matrix, user access register, backup schedule, restoration test evidence, business continuity plan, disaster recovery plan, incident response procedure, monitoring and logging evidence and change-management procedure.

Website evidence shall include domain / alias / redirect register, homepage screenshot, licence / seal display screenshot, registration screenshots, Terms and Conditions acceptance screenshots, current Terms and Conditions, Terms and Conditions version and archive, Privacy Notice, payment page screenshots, crypto warning screenshots, responsible gaming page screenshots, complaints page screenshots, ADR disclosure screenshots, bonus / promotion screenshots and website change-control records.

Supplier evidence shall include supplier register, due diligence files, criticality classification, supplier agreements, supplier responsibility matrix, Digitain evidence, Sumsb evidence, payment provider documentation, Spinmatic agreement, CoinPayments agreement, hosting agreement, EGIS-FZCO ADR terms, affiliate register, supplier monitoring records, incident records and exit plans. Training evidence shall include training policy, calendar, register, materials, attendance, effectiveness records and supplier training evidence.

## **18.7 Evidence Storage, Review and Critical Gaps**

The Company shall store evidence in a secure and organised evidence repository structured by corporate and licence, product and games, payments and crypto, AML / KYC, sanctions, responsible gaming, complaints and ADR, technical infrastructure, website and Terms and Conditions, suppliers, training, incidents and reports and Board approvals.

The evidence schedule shall be reviewed at least annually, before submission of the Manual to a regulator, before Board approval, following material operational changes, following supplier changes, following incidents, following audit findings and following regulatory requests. Outstanding gaps must be entered into the Implementation Action Tracker.

Critical evidence gaps include current licence certificate and conditions, current Terms and Conditions, ADR disclosure, Tier-IV Curaçao data centre evidence, CGA data availability mechanism, technical infrastructure diagram, Digitain agreement and matrix, product and game certification, Sumsb configuration, transaction monitoring rules, goAML readiness, sanctions procedure and frozen asset register, Spinmatic and CoinPayments agreements, crypto policy update for USDC and active networks, responsible gaming evidence, complaint channel, supplier register, reporting calendar and training register.

## Records and Evidence

| Record / evidence item                  | Status                 |
|-----------------------------------------|------------------------|
| Evidence repository                     | Available              |
| Evidence folder structure               | Available              |
| Evidence owner                          | Available              |
| Evidence access-control list            | Available              |
| Evidence review schedule                | Available              |
| Evidence gap log                        | Available              |
| Implementation Action Tracker           | Included in Section 19 |
| Critical evidence gap escalation record | Available              |

## 19. Implementation Action Tracker

This section consolidates the unresolved items in the Manual into a single Company confirmation and implementation tracker. The purpose of the tracker is to make it clear which confirmations, documents, procedures, screenshots, supplier evidence and implementation actions are required before the Manual can be treated as final, Board-approved or regulator-ready.

The tracker should be maintained by the MLRO / Compliance Officer and reviewed with senior management until all Critical items have been closed, formally risk-accepted or escalated. Closure of an item requires evidence, not only a verbal confirmation.

| Section | Action / information required                                                                                                                              | Status     | Priority | Owner       | Target date | Evidence / comments |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|----------|-------------|-------------|---------------------|
| 1       | Effective date and version                                                                                                                                 | 30/07/2026 | High     | Oxilium N.V |             | Version 1.1         |
| 1       | Final approval authority                                                                                                                                   | Approved   | High     | Management  |             |                     |
| 16      | Confirm CGA inspection production process, five-working-day availability, reporting calendar and 15 June / 15 January reporting deadlines where applicable | TBC        | Critical | Oxilium N.V | TBC         | TBC                 |

|    |                                                                                                                                                                                                |     |      |             |            |     |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------|-------------|------------|-----|
| 17 | Confirm annual training programme covers LOK/CGA topics including mental well-being, anti-bribery, crime prevention, responsible gaming, AML, player communication and responsible advertising | TBC | High | Oxilium N.V | 27/12/2026 | TBC |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------|-------------|------------|-----|

### 19.1 Critical Closure Principles

Critical items must be resolved before the Manual is used as a final regulatory or Board-approved document unless the Board expressly approves the Manual subject to documented conditions and interim controls. Critical items include licence evidence, Terms and Conditions, ADR disclosure, Tier-IV Curaçao data centre evidence, CGA data availability, key supplier agreements, product certification, Sumsu configuration, goAML readiness, sanctions freezing process, crypto policy updates and core compliance registers.

Where a Critical item cannot be closed immediately, the responsible owner must document the reason, interim control, target closure date, risk assessment and escalation decision. The Manual must then continue to show the item as **TBC / Action Required** until the evidence has been received and reviewed.

### 19.2 Company Sign-Off

| Field                    | Details         |
|--------------------------|-----------------|
| Reviewed and Approved by | Christiana Ilia |
| Role                     | CEO             |
| Date                     | 04/08/2026      |