

OPERATIONS MANUAL (OM) FOR ALPHA GAMES N.V.

1. GOVERNANCE, ROLES AND ACCOUNTABILITY

1.1 Board and Executive Oversight

- **Board responsibilities:**

- Approve and sign the OM
- Set risk appetite
- Approve annual compliance budget
- Receive quarterly compliance, AML, security, and audit reports.

The Board must meet at least quarterly and convene extraordinary meetings for material incidents.

- **CEO responsibilities:**

- Ultimate license compliance owner
- Ensure resources for compliance
- Sign off on major vendor contracts and material policy changes.

- **Reporting lines:**

- Compliance Officer reports functionally to the Board and operationally to the CEO
- CTO reports to CEO

1.2 Key Roles and detailed duties

- **Compliance Officer (CO):**

- Maintain OM
- Run AML/CFT program
- KYC policy owner
- File Suspicious Transaction Reports (STRs) to Curaçao authorities
- Maintain sanctions screening
- Conduct periodic AML risk assessments and maintain training logs.

- **Chief Technology Officer (CTO):**

- Platform integrity owner
- Responsible for secure architecture, patch management, encryption, backups, access control, vulnerability management, and incident response
- CTO approves technical change control and signs off on security attestations from vendors.

- **Finance / CFO:**

- Financial controls, AML transaction monitoring oversight, reconciliation, and suspicious payment escalation
- **Vendor Manager:**
 - Contract lifecycle, due diligence, SLA monitoring, and periodic vendor audits.

1.3 Delegation and Escalation Matrix

- Documented matrix showing decision thresholds for refunds, chargebacks, account closures, and suspicious activity escalations. All material decisions above defined monetary or reputational thresholds require Board notification within 72 hours.

1.4 Operational Ownership

This Operational Manual is owned, maintained, and periodically updated by the departments responsible for conducting the licensed operations to ensure it accurately reflects current business practices. While Compliance assists in regulatory alignment, the responsibility for describing processes remains with the operational, technical, customer support, and management functions.

- **Gaming Operations:** Managed by the Head of Operations and platform providers on a continuous basis via platform procedures, evidenced by platform documentation.
- **Quality Assurance:** Managed by the CTO and testing providers periodically via testing procedures, evidenced by test reports.
- **Player Protection:** Managed by the Compliance Officer and Operations continuously via platform controls, evidenced by Responsible Gaming (RG) reports.
- **Data Management:** Managed by the CTO and IT providers continuously via storage and retention policies, evidenced by retention records.

1.5 Purpose and Scope of Gaming Operation

- This manual outlines the internally managed and outsourced activities that support the delivery of Alpha Games N.V.'s licensed gaming operation.
- The licensed operator on its platform offers following a gaming categories: Slots, Live casino, Crash games, Bingo, Arcade and Mine, Table games. Outcomes are determined via certified RNG. The player journey begins with registration, proceeds through KYC verification, and allows for gameplay after the card or crypto deposit. Payouts are processed via card or crypto payment providers and are subject to internal transaction monitoring and fraud review.

2 REGULATORY FRAMEWORK, POLICIES AND COMPLIANCE PROGRAM

2.1 Regulatory Basis and Obligations

- The OM maps to LOK Article 5.9 requirements for an operations manual describing internal controls, reporting lines, and procedures. The OM also implements Curaçao AML/CFT rules, data protection obligations, and the Curaçao Gaming Authority (CGA) reporting expectations.

2.2 Core policies

- **Anti-Money Laundering Policy (CO):**
 - Annual review
 - Immediate update on regulatory change
- **KYC and Customer Due Diligence Policy (CO):**
 - Defines risk tiers, documentation requirements, EDD triggers, PEP handling, and source of funds verification.
- **Responsible Gaming Policy:**
 - Self-exclusion, deposit/time limits, cooling-off
 - VIP governance and referral procedures.
- **Data Protection and Privacy Policy (CTO/CO):**
 - Data minimization, retention, encryption, and breach notification timelines.
- **Game Integrity and RNG Policy (CTO):**
 - Provider certification, RTP monitoring, and game change control.
- **Incident Response and Business Continuity Policy (CTO/CO):**
 - Incident classification, notification timelines, and recovery objectives.

2.3 Compliance Program Elements

- **Risk assessment:**
 - Annual enterprise AML and operational risk assessment with documented mitigation plans.
- **Monitoring and Testing:**
 - Daily automated transaction monitoring, weekly rule tuning, monthly exception reviews, quarterly independent AML testing, and annual external audit.
- **Training:**
 - Mandatory onboarding and quarterly refresher training for AML, RG, and security. Training completion tracked in LMS.

3 CUSTOMER LIFECYCLE CONTROLS

3.1 Onboarding and KYC Procedures

- **Risk tiering:**
 - *Low risk:* Basic registration, email verification, phone verification for small deposit thresholds.
 - *Medium risk:* ID document (passport/ID card), proof of address dated within 3 months, payment method verification.
 - *High risk:* Full EDD including source of funds, employment verification, enhanced monitoring, and senior compliance approval.
- **Automated checks:**
 - Sanctions and PEP screening at registration and daily thereafter
 - Geolocation and IP checks to block prohibited jurisdictions.
- **KYC workflow:**
 - Automated document upload
 - OCR and liveness checks
 - Manual review SLA 24 hours
 - Escalation to CO for discrepancies.
- **Account activation:**
 - Conditional activation with deposit limits until KYC completed
 - Unverified accounts limited to low deposit/withdrawal thresholds.
- **Restricted Persons Controls:**
 - The operation prevents participation by prohibited individuals through automated age verification controls, self-exclusion arrangements, jurisdictional IP restrictions, and strict maintenance of exclusion lists.
 - Account monitoring measures escalate any attempted breaches directly to the Compliance Officer.
 - To support secure onboarding, automated document uploads are paired with ID validation and liveness checks to immediately filter out restricted individuals.

3.2 Ongoing Monitoring and Transaction Controls

- **Transaction monitoring rules:**
 - Limited EDD is a targeted, automated safety check triggered when a player crosses a specific behavioral limit but isn't doing anything obviously illegal.

- Instead of a full financial audit, it focuses strictly on a real-time ID Double-Check (verifying the tax ID is active) and an automated Sanctions and PEP check to confirm the user hasn't landed on a government blacklist.
- **Alerts and triage:**
 - Alerts categorized by severity:
 - ✓ low severity handled by Operations
 - ✓ medium escalated to Compliance
 - ✓ high severity immediate freeze and CO notification.
- **Suspicious activity reporting:**
 - STR template, evidence pack, and submission timelines to Curaçao authorities
 - All STRs logged and retained

3.3 Payments, Withdrawals and Chargebacks

- **Approved payment methods:**
 - Documented list with AML risk rating for each method
 - Dual-provider redundancy for banking and payment processing to mitigate interruptions.
- **Withdrawal controls:**
 - Identity re-verification for withdrawals above thresholds
 - Manual review for large or unusual withdrawals
 - Source of funds checks for large wins.
- **Chargeback handling:**
 - Reconciliation process,
 - Evidence collection
 - Dispute escalation to legal counsel.

3.4 Website and Player Interface:

- The visual and operational elements presented to players include a streamlined registration process utilizing partial biometric validation, secure account access portals, and direct interfaces for deposits and withdrawals.
- The dashboard provides immediate access to Responsible Gaming tools, game selection, account management features, and visible complaint submission channels

4 PLATFORM, SECURITY AND GAME INTEGRITY

4.1 Platform Architecture and Technical Controls

- **Platform components:**
 - Core (player accounts, balances, transactions, game sessions)
 - Admin panel (visual and API)

- Integrations running on separate servers. All integrations isolated by network segmentation.
- **Development and deployment:**
 - Secure SDLC, code reviews, automated testing, staging environment, and documented rollback procedures
 - Change control board approval required for production changes
- **Testing and Quality Assurance**
 - Beyond secure SDLC, the CTO oversees formal game certification processes, release and deployment testing, defect management, and periodic reviews. Testing is performed continuously during deployment windows, with critical defect findings addressed prior to production release

4.2 Security Controls and Standards

- **Access control:**
 - Role-based access control, least privilege, MFA for all privileged accounts, periodic access reviews.
- **Encryption:**
 - TLS for data in transit
 - AES-256 for sensitive data at rest
 - Key management policy.
- **Logging and monitoring:**
 - Centralized SIEM ingesting application, database, and network logs
 - Retention per policy.
- **Vulnerability management:**
 - Monthly scanning, quarterly penetration testing by accredited third parties, and patching SLAs.
- **Player Data Management:**
 - Player information, including KYC categories, gaming histories, and financial records is securely collected and retained.
 - The IT department governs storage arrangements, backup procedures, strict access controls, and verified deletion procedures aligned with the Information Security Policy.

4.3 Game Integrity and Provider Management

- **Provider due diligence:**
 - Verify provider licenses, RNG certification, RTP documentation, and independent test lab reports before integration
 - Maintain a provider register with certification expiry dates
- **Game session and event logging:**

- Store game events, sessions, and round outcomes in immutable logs with cryptographic integrity checks
- Retain logs per regulator retention schedule.
- **RTP and anomaly monitoring:**
 - Daily RTP reconciliation, statistical anomaly detection, and immediate investigation of deviations.

4.4 Incident Response and Business Continuity

To ensure operational resilience, we maintain a formal Business Continuity and Disaster Recovery (BCDR) plan that addresses the following key areas:

- **Critical Operational Functions:** We identify the Gaming Core (account management and transaction processing), Payment Gateways, and Customer Support channels as critical operational functions that must be maintained to ensure the integrity of the licensed operation.
- **Contingency Procedures:** In the event of a technical or operational disruption, we execute predefined contingency procedures, including manual failover to secondary processing environments, to ensure service continuity.
- **Disaster Recovery (DR) Arrangements:** Our DR strategy utilizes Cloud-based hot-standby to ensure a Recovery Time Objective (RTO) ASAP and a Recovery Point Objective (RPO) also ASAP. This ensures that operational data is restored following any significant incident.
- **Recovery Responsibilities:** The CTO holds ultimate responsibility for technical restoration, while the Head of Operations oversees service restoration and the resumption of normal player-facing activities.
- **Communication Procedures:** Internal communication is managed via Encrypted Internal Channel, while regulatory notifications regarding material incidents are triggered in accordance with the regulatory reporting matrix.
- **Escalation Arrangements:** Incidents are classified as Severity 1 (Critical), 2 (Major), or 3 (Minor). Severity 1 incidents trigger immediate escalation to the Board and the CGA within 24 hours of detection.
- **Testing and Review Activities:** The BCDR plan is subject to periodic testing to maintain operational resilience. Full-scale disaster recovery simulations are conducted annually, while critical system backups are validated monthly. Findings from these tests are documented in a Post-Test Report and reviewed by the CTO and Compliance Officer to refine recovery objectives and procedures.

4.5 Technical Infrastructure and Hosting:

- The technical environment is supported by AWS, utilizing a multi-region deployment to ensure high availability and optimal performance for the gaming platform. Our network architecture is structured with segmented, isolated VLANs for production, staging, and internal administrative management, providing secure access control and traffic management
- Systems are monitored on a 24/7 basis using **Cloudwatch + Grafana + Tick stack + ELK** which tracks traffic patterns, server health, and identifies potential security events in real-time.
- Data Centre arrangements are maintained with **Flutter Networks N.V.** which addresses Tier IV requirements by ensuring the following:
 - ✓ **Redundancy Measures:** The architecture employs N+1 redundancy for power and cooling, combined with fully redundant network paths to prevent single points of failure.
 - ✓ **Backup Locations:** Critical gaming and player transaction records are backed up daily to a geographically separate location where the service provider is located. These backups are stored using immutable policies to prevent unauthorized alteration or deletion.
 - ✓ **Restoration Capabilities:** Business continuity is supported by documented failover procedures. Full system restoration capabilities are tested and verified on a quarterly basis to ensure defined recovery objectives are met.
- All hosting agreements, service level agreements (SLAs), and relevant Data Centre certifications (e.g., ISO 27001, SOC 2, or specific Tier IV compliance documentation) are maintained in the corporate Vendor Management repository and are available for regulatory review upon request.

5 RESPONSIBLE GAMING, PLAYER PROTECTION AND COMPLAINTS

5.1 Responsible Gaming Tools and Processes

- **Player controls:**
 - Deposit limits, loss limits, session time reminders, self-exclusion, cooling-off, and reality checks
 - Limits adjustable by player with cooling-off delays for increases
 - Implemented responsible gaming principles encompass automated and manual player protection measures, including hard deposit limits, loss limits, self-exclusion functionality, and mandatory reality checks.

- Ongoing behavioral monitoring triggers structured escalation and intervention procedures.
- **Vulnerability detection:**
 - Player risk scoring using behavioral analytics to detect chasing losses, erratic play, or signs of problem gambling
 - High-risk players receive outreach and mandatory cooling-off offers
- **VIP governance:**
 - Separate VIP policy with enhanced affordability checks, documented approvals for credit or high-value offers, and senior compliance oversight

5.2 Complaints Handling

The operation manages player complaints and disputes through the following structured process, ensuring accountability and fairness:

- **Complaint Submission Methods:** Players may submit complaints via email support, or dedicated web form. Every submission is automatically assigned a unique ticket ID for end-to-end tracking within our CRM system.
- **Investigation Procedures:** All complaints undergo a triage process within 24 hours to categorize the issue (e.g., technical, financial, or service-related). The investigation involves gathering documented evidence from relevant systems, including game logs, transaction history, and prior communication records.
- **Escalation Routes:** Complaints not resolved at the initial support level are escalated to the Customer Support.
- **Response Timeframes:** We adhere to strict SLAs, providing an initial acknowledgment within 24 hours and aiming for full resolution within 7 business days of the initial submission.
- **Recordkeeping Arrangements:** All complaints are logged in a centralized Complaint Register, which includes the player identity, nature of the complaint, investigation notes, and final resolution. These records are protected against alteration and retained for 7 years, in alignment with our corporate retention policy.
- **Management Oversight:** The Head of Operations conducts a quarterly analysis of the Complaint Register to identify systemic issues or recurring defects. Findings, along with any necessary remediation plans, are reported directly to the Board to ensure continuous improvement of the gaming operation.

5.3 Terms and Conditions:

- The most recent version of the Terms and Conditions is perpetually accessible on the player interface.
- Updates undergo a strict approval process by the Legal Department, with version control arrangements, review procedures, and standardized update communication procedures ensuring players are informed of material changes.

6 AUDIT AND RECORDKEEPING

6.1 Internal and External Audit

- **Internal audit:**
 - Annual internal audit program covering AML, KYC, payments, game integrity, and IT security
 - Findings tracked to closure.
- **External audit:**
 - Annual independent audit of financials and compliance
 - Periodic independent testing of AML program and technical security.

6.2 Record Keeping and Retention

- **Record Keeping and Critical Information**
 - Operational records including player records, gaming transaction records, financial transaction records, audit logs, and account activity records are maintained securely.
 - All records feature protection against loss or alteration and are stored within secure database environments.
 - Responsibility for record maintenance falls to the Operations and IT departments, ensuring critical information remains easily accessible for regulatory review and data retrieval requests
- **Data retrieval**
 - Is managed by the IT department upon receipt of a formal request from the Regulator or an authorized internal auditor. Records are retrieved by querying the immutable audit log database or accessing the secure cloud archive
 - The retrieval process ensures the integrity of the data is maintained through checksum verification, and the output is provided in encrypted PDF or CSV format within 7 days of the request

APPENDICES

Appendix A: Definitions and Abbreviations

- **AML:** Anti-Money Laundering.
- **CDD:** Customer Due Diligence.
- **EDD:** Enhanced Due Diligence.
- **LOK:** Landsverordening op de Kansspelen (National Ordinance on Games of Chance).
- **RTP:** Return to Player.
- **STR:** Suspicious Transaction Report.
- **CGA:** Curaçao Gaming Authority.

Appendix B: KYC Tiers and Required Documents

- **Low risk:** Email, phone, IP geolocation check.
- **Medium risk:** Government ID; proof of address (utility bill or bank statement within 3 months); payment method verification.
- **High risk:** Source of funds documentation (bank statements, payslips), employer verification, enhanced monitoring plan, senior compliance approval.

Appendix C: Transaction Monitoring Rules Catalogue

- Deposit velocity, more than 5 deposits in 24 hours triggers review.
- Deposit/withdrawal ratio, deposits > 10x withdrawals in 7 days triggers review.
- Cross-account link same device or payment instrument used by multiple accounts triggers review.
- Large withdrawal withdrawals > €10,000 require EDD and CFO sign-off.

Appendix D: Incident Response Templates

- **Incident classification form** with fields for timeline, affected systems, initial containment steps, evidence preservation checklist, and notification list.
- **Regulator notification template** with incident summary, impact, remediation steps, and timeline.

Appendix E: STR and Regulatory Reporting Templates

- **STR template** with structured fields:
 - Subject details, transaction details, reason for suspicion, evidence attachments, and CO sign-off.
- **Regulatory reporting log** to track:
 - Submission dates, reference numbers, and follow-up actions.

Appendix F: Vendor Due Diligence Checklist

- Corporate registration and beneficial ownership.
- Financial statements and credit checks.
- Security certifications (SOC2/ISO27001).
- AML policy and KYC procedures.
- References and prior client list.
- Contractual clauses required.

Appendix G: Change Control and Release Checklist

- Change description, risk assessment, test results, rollback plan, approvals (CTO, CO, Head of Ops), scheduled window, and post-release verification checklist

Appendix H: Training Matrix and Records Template

- Role, mandatory modules, frequency, completion date, and assessment score. LMS export template for regulator review.

Appendix I: Record Retention Schedule

- KYC documents: minimum 7 years after account closure.
- Transaction logs: minimum 7 years.
- Game event logs: minimum 5 years.
- STRs and related correspondence: minimum 10 years.