

Purple Bay B.V.

Operations Manual

Curacao Online Gaming Operator

Document reference: PPB-OPS-MAN-001

Version: 1.0

Effective date: 11th June 2025

Approved by: Alexandre Etienne Assouline, CEO

Confidential — for internal and regulatory use only

Document Control

This Operations Manual (the “Manual”) is a controlled document. The master copy is held by the Compliance Officer of Purple Bay B.V. Distribution outside the PPB group is permitted only with the written approval of the CEO and Compliance Officer.

Version history

Version	Date	Author	Summary of changes	Approved by
1.0	11th June 2025	Compliance Officer	Initial issue	Alexandre Etienne Assouline, CEO
1.1	25th May 2026	Compliance Officer	Updated Version	Alexandre Etienne Assouline, CEO

Review cycle

The Manual is reviewed at least annually, and additionally whenever a material change occurs in the Company’s licence conditions, applicable law, corporate structure, outsourcing arrangements or operational model. Each section may be amended independently; any amendment is recorded in the version history above and the relevant section dated.

Distribution list

- Board of Directors, Xecutive Corporate Management B.V.
- CEO, Alexandre Etienne Assouline.
- CTO Consultant (Alexandre Etienne Assouline)
- Money Laundering Reporting Officer (MLRO) — {{Everhona Makaya}}
- Compliance Officer — {{Stacey-Lee Portillo}}
- Data Protection Officer — {{Stacey-Lee Portillo}}
- Responsible Gambling Officer — {{Pierre Flermoen}}
- Curaçao Local Representative / Key Person — {{Stacey-Lee Portillo}}
- Executive leadership, ServHGR Ltd — Aleksej Hugo Ander
- Curaçao Gaming Authority (on request)

Table of Contents

Document Control	2
Version history	2
Review cycle	2
Distribution list	2
Table of Contents	3
1. Company Overview	6
1.1 Company history	6
1.2 Mission, vision and values	6
Mission	6
Vision	6
Core values	6
1.3 Corporate structure	7
1.4 Licensing and regulatory framework	7
1.5 Restricted and prohibited territories	8
2. Governance and Organisation	9
2.1 Board and management	9
2.2 Roles and accountability matrix	9
2.3 Meetings and decision rhythm	10
2.4 Outsourcing oversight	10
2.5 Three lines of defence	10
3. Daily Operational Processes	12
SOP-3.01 — Start-of-day Operational Checks	12
SOP-3.02 — Player Registration and KYC Review	12
SOP-3.03 — Deposit Processing and Monitoring	13
SOP-3.04 — Withdrawal Processing and Approval	14
SOP-3.05 — Transaction Monitoring and AML Alerts	15
SOP-3.06 — Fraud Queue Handling	15
SOP-3.07 — Responsible Gambling Review	16
SOP-3.08 — Customer Support Shift Handover	17
SOP-3.09 — Bonus Issuance and Abuse Review	18
SOP-3.10 — Platform and Game Integrity Monitoring	18
SOP-3.11 — Affiliate Activity Review	19
SOP-3.12 — Daily PSP Reconciliation and Cash Position	20
SOP-3.13 — Complaints Triage and ADR Escalation	20
SOP-3.14 — Sanctions and PEP Daily Delta Screening	21
SOP-3.15 — Incident Response and Reporting	21

SOP-3.16 — End-of-day Operational Reporting	22
4. Policies and Guidelines	24
POL-4.01 — Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT)	24
POL-4.02 — Know-Your-Customer and Customer Due Diligence.....	24
POL-4.03 — Responsible Gambling and Player Protection	25
POL-4.04 — Complaints Handling and Alternative Dispute Resolution	25
POL-4.05 — Bonus, Promotions and Marketing.....	26
POL-4.06 — Data Protection and Privacy	26
POL-4.07 — Information Security.....	27
POL-4.08 — Business Continuity and Disaster Recovery.....	28
POL-4.09 — Player Funds Protection	28
POL-4.10 — Game Fairness and Random Number Generation.....	29
POL-4.11 — Outsourcing	29
POL-4.12 — Conflicts of Interest	29
POL-4.13 — Sanctions	30
POL-4.14 — Affiliate Standards	30
POL-4.15 — Workplace Conduct, Health and Safety.....	31
POL-4.16 — Whistleblowing.....	31
POL-4.17 — Record Retention.....	32
5. Quality, Control and Assurance Framework.....	33
5.1 Internal control statement	33
5.2 Key risk indicators (KRIs)	33
5.3 Internal audit	33
5.4 Independent third-party testing.....	33
5.5 Continuous improvement	33
6. Safety and Player Protection	34
6.1 Underage gambling prevention.....	34
6.2 Self-exclusion.....	34
6.3 Player-imposed limits and reality checks	34
6.4 Identifying and supporting at-risk players.....	34
6.5 Marketing safeguards.....	34
7. Contact Information	36
7.1 Internal contacts — Purple Bay B.V.....	36
7.2 ServHGR Ltd contacts	Error! Bookmark not defined.
7.3 Regulator	36
7.4 Alternative Dispute Resolution (ADR) for players	36
7.5 Financial Intelligence Unit	37
7.6 Key external service providers	37

Annex A — Glossary 38

Annex B — Document Review Log 39

Annex C — Restricted and Prohibited Territories 40

Annex D — Reference List of Laws and Regulations 41

1. Company Overview

1.1 Company history

Purple Bay B.V. (“Purple Bay” or “the Company”) is a private limited liability company incorporated under the laws of Curaçao, with its registered office at Korporaalweg 10, Willemstad, Curaçao, and entered in the Curaçao Chamber of Commerce under number 157944.

The Company is a wholly-owned subsidiary of Caramel Holding B.V., ultimately owned by Mr. Kaurah Harbinder Singh (the Ultimate Beneficial Owner). Purple Bay B.V. was established to act as the licensed operator of the group’s online gaming offering and holds an interactive gaming licence issued by the Curaçao Gaming Authority (“CGA”) under licence number OGL/2024/1368/0895, dated 23/05/2025, valid until 23/Jun/2026.

Since incorporation the Company has focused on building a multi-vertical online gaming proposition (casino, live casino and selected complementary verticals) supplied through integrations with regulated third-party game studios and aggregators. The Company does not develop core games in-house; it operates as a licensed B2C operator on top of certified gaming content.

Operational delivery is provided through a service agreement with ServHGR Ltd., which supplies customer support, customer relationship management (CRM), payments operations, and risk and fraud services to Purple Bay B.V. The outsourcing arrangement is governed by a written service agreement and the outsourcing oversight framework set out in Section 4.11 of this Manual.

1.2 Mission, vision and values

Mission

To provide a safe, fair and entertaining online gaming experience to adult players in the markets in which the Company is licensed to operate, while upholding the highest standards of player protection, regulatory compliance and operational integrity.

Vision

To be regarded by players, partners and regulators as a trustworthy and technically excellent Curaçao-licensed operator, demonstrating that the post-2024 Curaçao licensing framework can produce operators of an international standard.

Core values

- Player first — every operational decision is tested against the question, “Does this protect or enhance the player’s experience?”
- Integrity over short-term gain — we do not chase revenue at the cost of compliance, fair gaming or responsible gambling commitments.
- Transparency — players, partners and regulators receive accurate information, on time, in plain language.
- Accountability — every process has a named owner; every decision is documented; every incident is recorded.

- Continuous improvement — we treat regulatory change, audit findings and player feedback as inputs to a recurring improvement cycle, not one-off events.

1.3 Corporate structure

The Company's position within the wider PPB group is summarised below:

Entity	Jurisdiction	Role	Relationship
Caramel Holding B.V.	Curaçao	Holding company	100% owner of Purple Bay B.V.
Purple Bay B.V.	Curaçao	Licensed online gaming operator	Subject entity of this Manual
ServHGR Ltd.	Malta	Outsourced service provider (CS, CRM, payments operations, risk and fraud)	Group affiliate under common control; contracted under MSA dated

The Ultimate Beneficial Owner (UBO) of Caramel Holding B.V. is Mr. Kaurah Harbinder Singh, and the UBO of ServHGR Ltd is Mr. Aleksej Hugo Ander. The respective UBOs are recorded in the Curaçao UBO Register in accordance with the National Ordinance on UBO Registration.

1.4 Licensing and regulatory framework

Purple Bay B.V. is licensed and supervised by the Curaçao Gaming Authority. The Company is subject to and complies with, among others, the following primary instruments:

- Landsverordening op de Kansspelen (LOK) — National Ordinance on Games of Chance, as amended.
- Subsidiary regulations, licence conditions and directives issued by the Curaçao Gaming Authority, including Responsible Gaming, Player Protection, AML/CFT and Technical Standards directives.
- Landsverordening Identificatie bij Dienstverlening (LID) — National Ordinance on Identification when Rendering Services.
- Landsverordening Melding Ongebruikelijke Transacties (LMOT) — National Ordinance on the Reporting of Unusual Transactions, including reporting to the Financial Intelligence Unit (Meldpunt Ongebruikelijke Transacties, "FIU Curaçao").
- National Ordinance on the Penalisation of Money Laundering and Terrorist Financing.
- National Ordinance on the Protection of Personal Data and, where applicable to EU/EEA data subjects, Regulation (EU) 2016/679 (GDPR).
- Applicable economic sanctions regimes (UN, EU, OFAC and any locally implemented sanctions).

In each market in which the Company accepts players, the Company complies with applicable local restrictions, including geo-blocking of restricted territories listed in Annex C.

1.5 Restricted and prohibited territories

The Company does not knowingly accept registrations or wagers from, and applies geo-IP and KYC-based blocking to, residents of the territories listed in Annex C. The list is reviewed at least quarterly by the Compliance Officer and updated whenever a change in law, licensing condition or group risk appetite requires it.

2. Governance and Organisation

2.1 Board and management

Ultimate responsibility for the Company rests with the Board of Directors of Purple Bay B.V. The Board meets at least quarterly and is responsible for approving the strategy, risk appetite, annual budget, this Manual, and the appointment of key persons.

Day-to-day management is delegated to the Chief Executive Officer, who chairs the Executive Committee. The Executive Committee meets at least monthly and is composed of:

- Chief Executive Officer (CEO) — Alexandre Etienne Assouline
- Chief Technology Officer Consultant (CTO Consultant) — Alexandre Etienne Assouline
- Compliance Officer — Stacey-Lee Portillo
- Money Laundering Reporting Officer (MLRO) — Everhona Makaya
- Data Protection Officer (DPO) — Stacey-Lee Portillo
- Responsible Gambling Officer — Pierre Flermoen
- Curaçao Local Representative / Key Person — Stacey-Lee Portillo
- Head of Operations, ServHGR Ltd — Aleksej Hugo Ander

2.2 Roles and accountability matrix

The following accountability matrix sets out, for each operational domain, the responsible and accountable roles. Where a function is delivered by ServHGR Ltd under outsourcing, the ultimate accountability remains with Purple Bay BV.

Domain	Accountable (PPB)	Responsible (operational)
Strategy & risk appetite	CEO / Board	CEO
Technology platform	CEO	CTO Consultant
Compliance & licensing	CEO	Compliance Officer
AML/CFT, sanctions, FIU reporting	CEO	MLRO
Responsible gambling	Compliance Officer	RG Officer / HGR RG team
Data protection	CEO	DPO
Customer support	Compliance Officer	HGR Head of Customer Support
CRM and player communications	Compliance Officer	HGR Head of CRM
Payments operations & PSP relations	CEO	HGR Head of Payments
Risk and fraud operations	MLRO / Compliance Officer	HGR Head of Risk
Complaints handling	Compliance Officer	HGR Complaints Officer

Domain	Accountable (PPB)	Responsible (operational)
Affiliate compliance	Compliance Officer	HGR Head of CRM
Business continuity	CEO	CTO Consultant

2.3 Meetings and decision rhythm

Meeting	Frequency	Chair	Standing agenda
Board of Directors	Quarterly	Chair of the Board	Strategy, financials, key risks, regulator interactions, audit findings, approval of Manual amendments
Executive Committee	Monthly	CEO	Performance against KPIs, compliance dashboard, incident review, project status, regulatory horizon
Compliance & Risk Committee	Monthly	Compliance Officer	AML alerts and SARs, sanctions hits, RG cases, complaints trends, audit findings
Operations Daily Stand-up	Daily (business day)	HGR Duty Manager	Overnight events, open tickets, KPIs, blockers
Technology Review	Bi-weekly	CTO Consultant	Availability, incidents, change pipeline, security posture

2.4 Outsourcing oversight

Although a substantial portion of operational delivery is outsourced to ServHGR Ltd, Purple Bay B.V. remains the regulated entity and retains full responsibility for all outsourced activities towards the CGA and players.

Outsourcing is governed by:

- A written Master Services Agreement (MSA) between Purple Bay B.V. and ServHGR Ltd, including service descriptions, SLAs, audit rights, sub-outsourcing controls, data protection terms, business continuity obligations, and termination provisions.
- Quarterly outsourcing oversight reports from ServHGR Ltd to the Compliance Officer, covering SLA performance, material incidents, regulatory issues, control failures, and remediation.
- Right of audit exercisable by Purple Bay B.V. and, on request, the CGA and external auditors.
- An annual outsourcing risk assessment performed by the Compliance Officer and approved by the Board.

2.5 Three lines of defence

The Company applies a three-lines-of-defence model:

- First line — Business operations ServHGR Ltd teams and PPB commercial functions execute controls embedded in day-to-day processes.
- Second line — Compliance, MLRO, DPO and RG Officer provide independent oversight, advice, monitoring and challenge.
- Third line — Independent internal audit and external auditors (financial: Xecutive Corporate Management B.V) provide independent assurance to the Board.

3. Daily Operational Processes

This Section sets out the standard operating procedures (SOPs) that govern the daily running of Purple Bay B.V. Each SOP follows a common structure: owner, frequency, purpose, inputs, steps, outputs, escalation and key performance indicators. Where a process is delivered by ServHGR Ltd under outsourcing, the SOP applies to the HGR team as if it were an internal team, and the named PPB role retains accountability.

SOP-3.01 — Start-of-day Operational Checks

Field	Detail
Process owner	HGR Duty Manager (overseen by PPB CTO Consultant)
Frequency / trigger	Daily, 09:00 CET (or shift opening)
Purpose	Confirm platform, supplier and operational readiness before the active business day, and surface overnight issues for triage.

Inputs: Monitoring dashboards (platform, wallet, KYC, PSP, game studios), overnight incident log, overnight ticket queue, overnight AML/RG alert digests.

Steps:

1. Ping platform health endpoints: player wallet, registration, KYC integration, PSP gateway, game launcher.
2. Review overnight monitoring alerts and confirm any auto-remediated incidents are documented.
3. Inspect open P1/P2 incident tickets; confirm an owner is assigned and an ETA is communicated.
4. Confirm overnight automated reconciliation jobs (deposits, withdrawals, bonuses, GGR) completed successfully; investigate any failures within 30 minutes.
5. Review overnight RG flags and self-exclusion requests received outside business hours; ensure none are older than 2 hours without acknowledgement.
6. Confirm sanctions/PEP daily delta screening job has run; flag failures to Compliance Officer.
7. Publish the morning operations digest in the #ops channel and email distribution list.

Outputs / records: Start-of-day checklist (signed by Duty Manager), morning ops digest, list of open issues with owners.

Escalation: Any failed health check or unprocessed RG/self-exclusion request older than 2 hours → Compliance Officer and CTO Consultant immediately.

KPIs: 100% of checklist items completed by 09:30; zero unacknowledged RG/self-exclusion requests at start of day.

SOP-3.02 — Player Registration and KYC Review

Field	Detail
Process owner	ServHGR KYC Team Lead (oversight: Compliance Officer)
Frequency / trigger	Continuous; manual queue worked within 24 hours of arrival
Purpose	Verify the identity, age, residence and risk profile of every new player and apply the appropriate level of customer due diligence (CDD, SDD or EDD).

Inputs: Registration record, identity documents, proof of address (where required), KYC vendor results (Dilisense) sanctions/PEP screening results, IP/device data.

Steps:

8. On registration, run automated checks: minimum age (18 years), residence not on the restricted list, duplicate-account detection, sanctions/PEP screening.
9. Auto-approve players who pass all checks at low risk and complete biometric/document verification successfully; record decision in the KYC log.
10. Route to manual queue any player with: name mismatch, low-quality document, jurisdictional flag, PEP/sanctions partial match, multi-account signal, or risk score above the SDD threshold.
11. KYC Analyst reviews the case, requests additional documentation if needed (proof of address, source of funds for EDD), and records the rationale for the decision.
12. For EDD cases, escalate to MLRO before approving the account; EDD review must include documented source-of-funds assessment.
13. Apply the appropriate risk tier (Low / Medium / High) and propagate it to the transaction monitoring system.
14. Notify the player of the decision via the registered email channel within SLA.

Outputs / records: KYC decision record (with timestamps, reviewer, evidence references), risk tier assignment, sanctions/PEP screening evidence, retained identity documents (encrypted at rest).

Escalation: Confirmed sanctions hit → MLRO immediately (account frozen). EDD case unresolved > 5 business days → Compliance Officer.

KPIs: ≥ 95% of manual KYC cases closed within 24h; 100% of EDD cases documented with source-of-funds evidence; zero account openings with unresolved sanctions hits.

SOP-3.03 — Deposit Processing and Monitoring

Field	Detail
Process owner	ServHGR Payments Team
Frequency / trigger	Real-time
Purpose	Ensure every deposit is authorised, attributable to the verified account holder, and screened for fraud and money-laundering indicators.

Inputs: PSP authorisation responses (PaymentIQ orchestration layer), player KYC tier, transaction history, device/IP fingerprint, BIN country, blacklists.

Steps:

15. Block any deposit where the player account is suspended, self-excluded, or in EDD pending.
16. Verify that the payment instrument holder name matches the registered player name (or recorded acceptable alias); reject mismatches and flag for review.
17. Run velocity, structuring and pattern rules; deposits matching a rule are placed on hold pending review.
18. Confirm BIN country alignment with registration country; deposits from prohibited or high-risk jurisdictions are declined.
19. For first deposit, confirm full KYC status before crediting the wallet.
20. Record the deposit in the platform ledger and PSP ledger; confirm both sides reconcile within the same trading day.

Outputs / records: PSP transaction log, deposit decision log with reason codes, fraud alerts created where applicable.

Escalation: Sanctioned-country card use or confirmed identity mismatch → MLRO. Repeated failures from the same PSP > 1% → Head of Payments and CTO Consultant.

KPIs: Auto-approval rate ≥ 90% on low-risk players; deposit-to-ledger reconciliation variance < 0.05% per day; zero deposits credited to suspended accounts.

SOP-3.04 — Withdrawal Processing and Approval

Field	Detail
Process owner	ServHGR Payments Team (4-eyes approval for amounts above threshold)
Frequency / trigger	Continuous; first review within 24 hours; payment within 48 hours of approval
Purpose	Ensure withdrawals are paid promptly to verified players using legitimate funds, while preventing fraud and money laundering.

Inputs: Withdrawal request, player KYC tier, wagering / bonus state, recent transaction pattern, PSP availability for the chosen method.

Steps:

21. Confirm KYC tier is sufficient for the requested amount; if not, request the additional documentation needed before processing.
22. Verify wagering requirements on any active bonus are fully met; reject or partially reduce per the Bonus Policy if not.
23. Apply the return-of-deposit rule: withdrawals must, where possible, return to the original deposit instrument(s) before any alternative payout method is used.
24. For amounts above EUR 2000, a second reviewer (different from the first) confirms the decision.
25. For amounts above EUR 5000 Senior Risk approval is required and documented.

26. Execute the payout via the appropriate PSP; record the transaction reference in the platform ledger.

27. Notify the player of the outcome via in-app and email.

Outputs / records: Withdrawal decision record with named approvers, payout reference, ledger entries.

Escalation: Suspected fraud → freeze withdrawal, open risk case, notify MLRO. Aged withdrawals (> 72h without payout) → Head of Payments and Compliance Officer.

KPIs: Median time-to-payout < 24h for verified players; rejection rate by reason code tracked weekly; zero withdrawals approved to sanctioned or self-excluded accounts.

SOP-3.05 — Transaction Monitoring and AML Alerts

Field	Detail
Process owner	MLRO (operational triage by SERVHGR LTD Risk Team)
Frequency / trigger	Continuous detection; daily review of alert queue
Purpose	Detect and report transactions and behavioural patterns that may indicate money laundering, terrorist financing or other financial crime.

Inputs: Player transaction history, deposit and withdrawal patterns, source-of-funds documentation, sanctions/PEP screening results, third-party intelligence.

Steps:

28. Run rule-based and behavioural-model alerts continuously across all live accounts.
29. HGR Risk analysts triage the alert queue daily and assign each alert a disposition: false positive, monitor, request information, EDD, or report.
30. Where disposition is to report, the MLRO is engaged within one business day; the MLRO assesses whether an unusual transaction report is to be filed with the FIU Curaçao under the LMOT.
31. All filings are made in the prescribed format, within the prescribed timeframe, and recorded in the SAR/STR register accessible only to the MLRO and CEO.
32. Tipping off the customer is strictly prohibited; relevant policies in Section 4.1 apply.

Outputs / records: Alert register, case files with evidence, SAR/STR register, FIU filing receipts.

Escalation: Any urgent matter (e.g. apparent terrorist financing) → MLRO and CEO immediately; FIU notified without delay.

KPIs: 100% of alerts triaged within 2 business days; 100% of decisions to file or not file documented; SAR/STR filed within the regulatory deadline in every case.

SOP-3.06 — Fraud Queue Handling

Field	Detail
Process owner	SERVHGR LTD Head of Risk

Field	Detail
Frequency / trigger	Continuous; daily queue review
Purpose	Identify and respond to fraud, abuse and collusion in a consistent, evidence-based way.

Inputs: Rule-engine alerts, chargeback notifications, device/IP analytics, bonus abuse signals, multi-accounting signals, third-party intelligence.

Steps:

33. Categorise each case: chargeback / promo abuse / multi-accounting / collusion / identity fraud / arbitrage / other.
34. Gather evidence (logs, screenshots, device fingerprints, payment data) and record in the case file.
35. Apply the action matrix: warn, limit, freeze, close, claw back bonus, refund, or refer to law enforcement.
36. Where the player has lost legitimate funds due to identity theft, coordinate with PSP and Compliance Officer to facilitate restitution.
37. Generate weekly trends report; recurring patterns are escalated to the Compliance & Risk Committee.

Outputs / records: Risk case file, action record, chargeback dispute pack where applicable, weekly trend report.

Escalation: Confirmed organised fraud or insider involvement → CEO and Compliance Officer immediately; consider regulator notification.

KPIs: Chargeback rate < 0.5% of deposits by value; fraud loss < 1,000 EUR of GGR; case closure time median < 5 days.

SOP-3.07 — Responsible Gambling Review

Field	Detail
Process owner	Responsible Gambling Officer (with ServHGR RG team)
Frequency / trigger	Daily review of flags and self-exclusion requests; continuous monitoring
Purpose	Identify and intervene with players who may be experiencing or at risk of gambling-related harm, and to action all RG tool requests promptly.

Inputs: RG behavioural model outputs, deposit/loss-limit change requests, self-exclusion requests, cooling-off requests, player communications, customer support escalations.

Steps:

38. Triage RG model flags by severity; engage with high-severity flags within 24 hours via the player's registered channels.

39. Process self-exclusion requests within 1 hour of receipt; ensure all marketing, bonuses and account access are suspended for the requested period.
40. Process deposit/loss-limit decreases immediately; deposit/loss-limit increases are subject to the regulatory cooling-off period before taking effect.
41. Where a player is identified as at-risk, offer signposting to professional support services and, where appropriate, impose protective limits or temporary suspension.
42. Maintain the RG case register and a separate self-exclusion register that is checked at registration and at every deposit attempt.
43. Brief HGR CS and CRM teams not to contact excluded or at-risk players for marketing purposes.

Outputs / records: RG case register, self-exclusion register, RG interventions log, RG monthly report to the Compliance & Risk Committee.

Escalation: Player at immediate risk of harm → RG Officer engages directly; Compliance Officer informed within the same business day.

KPIs: 100% of self-exclusion requests processed within 1 hour; zero marketing contact with excluded players; high-severity RG flags engaged within 24h.

SOP-3.08 — Customer Support Shift Handover

Field	Detail
Process owner	ServHGR Head of Customer Support
Frequency / trigger	Per shift change (24/7 operation)
Purpose	Ensure continuity of service, knowledge transfer, and accountability across rotating support shifts.

Inputs: Open ticket queue, incident bridge notes, RG/risk flags raised by CS during the shift, known platform issues.

Steps:

44. Outgoing shift lead summarises: open tickets needing follow-up, VIP issues, RG escalations raised, any platform issues observed.
45. Incoming shift lead acknowledges the handover and confirms staffing levels meet the published roster.
46. Quality lead performs a random sample review (5% minimum) of closed tickets from the prior shift, scoring against the CS QA rubric.
47. Tickets failing QA are returned for rework and feedback is captured in the agent's record.
48. Shift report is filed in the CS log.

Outputs / records: Shift handover log, QA scoring report, CS daily KPI extract.

Escalation: Staffing below threshold or unresolved P1 → Head of CS and Duty Manager.

KPIs: Median first response < 2 minutes (chat); median resolution < 4 hours; CSAT ≥ 90%; QA pass rate ≥ 95%.

SOP-3.09 — Bonus Issuance and Abuse Review

Field	Detail
Process owner	ServHGR Head of CRM (oversight: Compliance Officer)
Frequency / trigger	Daily campaign launches; daily abuse queue review
Purpose	Run promotional campaigns that comply with the Bonus and Marketing policies and prevent bonus abuse without unfairly disadvantaging legitimate players.

Inputs: Approved campaign briefs, eligibility rules, abuse rule outputs, deposit/wager data.

Steps:

49. Verify each new campaign has been approved by Compliance and meets the Bonus Policy (wagering, eligibility, max bet, game restrictions, expiry).
50. Publish only the approved variant; record campaign codes, eligibility, T&Cs, and budget cap.
51. Monitor live campaigns against the abuse rules: shared device/IP/payment instrument, abnormal bonus-to-deposit ratios, restricted game patterns.
52. Bonus abuse cases are reviewed; legitimate disputes are escalated to Complaints under SOP-3.13.
53. Where a bonus is clawed back, the rationale is recorded, communicated to the player and made available to the Compliance Officer.

Outputs / records: Campaign register, abuse case decisions, monthly bonus expense reconciliation.

Escalation: Material discrepancy between campaign budget and actual cost > 10% → Head of CRM and CFO function.

KPIs: Bonus cost to GGR ratio within budget; abuse rate below target; zero unapproved live campaigns.

SOP-3.10 — Platform and Game Integrity Monitoring

Field	Detail
Process owner	CTO Consultant (operational: ServHGR Platform Operations)
Frequency / trigger	Continuous (automated) plus daily review
Purpose	Ensure the gaming platform is available, the games delivered are certified and functioning correctly, and player-facing odds reflect the certified RTPs.

Inputs: Monitoring system, vendor status pages, RNG/RTP certificates, jackpot status feeds.

Steps:

54. Monitor uptime of platform, wallet, KYC, PSP and each game studio integration.

55. Confirm RNG and RTP certificates for each game in catalogue are valid; remove or hide games with expired certification.
56. Investigate any player-reported game anomaly within 4 hours; coordinate with the game studio and document the resolution.
57. Pause a game vertical or studio where a material integrity issue is suspected, after consultation with the Compliance Officer.
58. Maintain a register of game studio approvals and removals.

Outputs / records: Availability and incident reports, game catalogue change log, certification register.

Escalation: Material integrity incident → Compliance Officer (CGA notification considered); P1 outage → Incident Response (SOP-3.15).

KPIs: Platform uptime ≥ 99.9% monthly; zero games served with expired RNG certification; mean time to acknowledge game anomalies < 4h.

SOP-3.11 — Affiliate Activity Review

Field	Detail
Process owner	ServHGR Head of CRM (oversight: Compliance Officer)
Frequency / trigger	Daily traffic and quality review; monthly payout reconciliation
Purpose	Ensure that affiliate-driven acquisition complies with the Affiliate Policy and marketing standards, and that affiliates are not driving non-compliant or fraudulent traffic.

Inputs: MyAffiliates daily report, traffic source data, registration quality metrics, geo-IP data, marketing creative library.

Steps:

59. Review daily acquisition by affiliate; investigate unusual spikes, sudden geographic shifts or low-quality registrations.
60. Spot-check affiliate creatives for compliance: no targeting of minors, no implied guarantees, no targeting of restricted territories, RG and licence disclosures present.
61. Where breaches are identified, suspend the affiliate pending investigation and notify them in writing.
62. Monthly: reconcile payout calculations with the MyAffiliates platform and Finance's ledger.
63. Quarterly: review the affiliate book for concentration risk and counterparty due diligence updates.

Outputs / records: Affiliate traffic review log, creative review log, suspension/termination notices, monthly payout reconciliation.

Escalation: Suspected coordinated fraud or targeting of restricted markets → Compliance Officer immediately.

KPIs: 100% of new affiliates have completed due diligence; creative compliance $\geq 98\%$ on sample audits; affiliate-driven fraud rate $< 20\%$. This includes single depositors.

SOP-3.12 — Daily PSP Reconciliation and Cash Position

Field	Detail
Process owner	Finance (oversight: CEO)
Frequency / trigger	Daily, by 14:00 CET for the previous trading day
Purpose	Reconcile movements across each PSP and bank account against the platform ledger, and report the consolidated cash position.

Inputs: PSP statements (PaymentIQ feed plus individual PSP portals), bank statements, platform ledger extract, chargeback notifications.

Steps:

64. Pull PSP and bank statements for the previous trading day.
65. Match each transaction line to a platform ledger entry; identify and investigate any unmatched entries.
66. Confirm player funds held in the safeguarded account meet or exceed the aggregate player balance.
67. Produce the daily cash position report and circulate to CEO and CTO Consultant.
68. Escalate any variance $> 5\%$ or any breach of player-funds safeguarding.

Outputs / records: Daily reconciliation pack, cash position report, unresolved-items log.

Escalation: Player-funds shortfall → CEO and Compliance Officer immediately; CGA notification considered without delay.

KPIs: Reconciliation complete by 14:00 in $\geq 98\%$ of days; aged unmatched items > 5 business days = 0; zero days of player-funds shortfall.

SOP-3.13 — Complaints Triage and ADR Escalation

Field	Detail
Process owner	Complaints Officer (ServHGR)
Frequency / trigger	Continuous logging; Level 1 within 48h, Level 2 within 7 days
Purpose	Resolve player complaints fairly, consistently and within published timeframes, and signpost players to the designated ADR provider where appropriate.

Inputs: Complaints received via in-app, email, chat, social media or regulator referral.

Steps:

69. Log every complaint within 24 hours in the complaints register, with a unique reference and category.

70. Level 1: front-line CS attempts to resolve and responds within 48 hours.
71. Level 2: if the player is not satisfied, the complaint is escalated to the Complaints Officer, who must respond with a substantive decision within 7 calendar days (and in any event no later than 8 weeks from receipt).
72. If the player remains dissatisfied after Level 2, the Complaints Officer issues a final response letter and informs the player in writing of their right to refer the complaint to **{{ADR_PROVIDER}}**, the Company's designated Alternative Dispute Resolution provider.
73. Maintain the complaints register and produce a monthly complaints report (volume, category, root cause, time-to-resolve, ADR cases) for the Compliance & Risk Committee.

Outputs / records: Complaints register, final response letters, ADR submissions log, monthly complaints report.

Escalation: Regulator-referred complaint → Compliance Officer immediately and CEO notified.

KPIs: 100% of complaints logged within 24h; 100% acknowledged within 48h; ≥ 95% closed within 8 weeks; recurring root causes tracked to remediation.

SOP-3.14 — Sanctions and PEP Daily Delta Screening

Field	Detail
Process owner	Compliance Officer (operational: ServHGR Risk)
Frequency / trigger	Daily
Purpose	Re-screen the active player base against updated international sanctions and PEP lists to ensure no prohibited person is being served.

Inputs: Active player base, updated OFAC / EU / UN / UK / Curaçao sanctions lists, PEP lists, screening engine output.

Steps:

74. Run daily delta screening against the previous day's lists.
75. Triage hits: clear false positives with documented rationale; confirmed hits result in immediate account freeze and MLRO escalation.
76. Where a confirmed sanctions hit is made, halt all transactions on the account, do not pay out funds without legal advice, and notify the relevant authorities as required by law.
77. Record each hit, decision and supporting evidence in the screening register.

Outputs / records: Daily screening log, hit-resolution records, frozen-accounts register.

Escalation: Confirmed sanctions hit → MLRO, Compliance Officer and CEO immediately.

KPIs: 100% of active players re-screened daily; 100% of hits triaged within 24h; zero confirmed sanctioned-person transactions.

SOP-3.15 — Incident Response and Reporting

Field	Detail
Process owner	CTO Consultant (technical) / Compliance Officer (regulatory and player-impact)
Frequency / trigger	On demand
Purpose	Respond to operational, security and compliance incidents in a structured, documented way, and meet regulatory reporting obligations.

Inputs: Monitoring alerts, vendor notifications, player reports, internal observations, regulator communications.

Steps:

78. On detection, classify severity (S1–S4) using the published matrix and open an incident record.
79. Assemble the response team appropriate to the severity and incident type (technical, security, compliance, player).
80. Contain, eradicate and recover; communicate updates on a cadence appropriate to severity.
81. For S1/S2 incidents, the CEO is informed without delay; player-affecting incidents trigger pre-approved player communications.
82. Assess regulatory reporting obligations to the CGA and, where applicable, the FIU, data protection authority or law enforcement; report within the prescribed timeframe.
83. Conduct a post-incident review within 10 business days and capture lessons learned and remediation actions with owners and due dates.

Outputs / records: Incident record, communications log, regulator filings, post-incident review report.

Escalation: S1 → CEO and Compliance Officer immediately; data breach → DPO without delay.

KPIs: 100% of S1/S2 incidents have a post-incident review within 10 business days; 100% of regulatory deadlines met; reopen rate < 5%.

SOP-3.16 — End-of-day Operational Reporting

Field	Detail
Process owner	ServHGR Duty Manager
Frequency / trigger	Daily, end of business day CET
Purpose	Provide leadership with a concise, accurate end-of-day picture of operational performance, risk and compliance.

Inputs: Operational dashboards, KPI extracts, day's incident and complaint logs, AML/RG/fraud queue status.

Steps:

84. Compile the end-of-day digest with: deposits, withdrawals, GGR, NGR, registrations, KYC throughput, complaints volume and aging, AML alerts triaged, RG cases opened, fraud cases opened, incidents (with severity).

- 85. Highlight exceptions versus target and any open items requiring overnight attention.
- 86. Distribute to CEO, CTO Consultant, Compliance Officer, MLRO, RG Officer and HGR executive team.
- 87. Archive in the operational reporting library.

Outputs / records: Daily ops digest (PDF and structured data), archived in document management system.

Escalation: Material adverse exception → CEO same evening.

KPIs: Digest issued by 21:00 CET in $\geq 95\%$ of days; data accuracy $\geq 99\%$ on sample audits.

4. Policies and Guidelines

This Section sets out the Company's policies. Each policy is owned by a named role, applies to a defined scope, and is supported by controls embedded in the operational SOPs in Section 3. Each policy is reviewed at least annually and after any material change.

POL-4.01 — Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT)

Purpose: Prevent the use of the Company's products for money laundering, terrorist financing or other financial crime, and ensure full compliance with the LOK, LID, LMOT and applicable international standards.

Scope: All Purple Bay B.V. employees and consultants, all ServHGR Ltd personnel performing outsourced functions, and any agent or affiliate acting on behalf of the Company.

Policy owner: Money Laundering Reporting Officer (MLRO).

Key principles:

- A risk-based approach is applied to every customer relationship.
- No customer relationship is opened or continued where a sanctioned person is identified.
- The MLRO operates independently and has direct access to the Board.
- Tipping off a customer who is the subject of a report is prohibited.
- Records are retained for the statutory minimum of ten (10) years from the end of the customer relationship.

Key controls:

- Customer identification and verification at onboarding (CDD) with SDD for low-risk and EDD for high-risk profiles.
- Daily sanctions and PEP screening of the active player base (delta).
- Continuous transaction monitoring with rule-based and behavioural alerts.
- Source-of-funds and source-of-wealth checks above defined thresholds.
- Mandatory annual AML training for all relevant staff, with role-specific refreshers.
- Annual AML risk assessment approved by the Board.

Review cycle: Annually, or upon material legal or risk change.

POL-4.02 — Know-Your-Customer and Customer Due Diligence

Purpose: Ensure that the Company knows the identity, age, residence and risk profile of every player before any business relationship is entered into and throughout its life.

Scope: All player accounts and any related parties (e.g. beneficial owners where corporate accounts are relevant).

Policy owner: Compliance Officer.

Key principles:

- No anonymous accounts.

- Verification is performed using reliable, independent source documents, data or information.
- Ongoing due diligence is performed throughout the relationship, including periodic reviews based on risk.
- Players are treated fairly and informed clearly of the documents and information required.

Key controls:

- Identity verification through including biometric liveness and document authenticity checks.
- Age verification — accounts are not opened for persons under 18; any account discovered to belong to a minor is closed and funds returned per the Underage Policy.
- Residence verification (proof of address) above defined thresholds.
- Trigger-based re-verification: significant deposits/withdrawals, change of personal details, time-since-last-review, risk-tier change.
- Centralised KYC record retained for the statutory period.

Review cycle: Annually.

POL-4.03 — Responsible Gambling and Player Protection

Purpose: Provide a gaming environment that helps players keep their play within healthy limits and intervenes early where harm is suspected.

Scope: All player-facing channels (platform, marketing, customer support) and all employees and outsourced staff.

Policy owner: Responsible Gambling Officer.

Key principles:

- Gaming is for adults aged 18 or over.
- Players control their play: deposit, loss, wager and session limits are available to all players, with increases subject to a cooling-off period.
- Self-exclusion is honoured immediately and irrevocably for the chosen period.
- Excluded and at-risk players are not targeted with marketing.
- Staff are trained to recognise signs of harm and to escalate appropriately.

Key controls:

- RG tools: deposit limits, loss limits, wager limits, session time limits, reality checks, cooling-off, self-exclusion.
- Behavioural monitoring model to detect at-risk play.
- Player-facing information on safer gambling and links to professional support services.
- Marketing suppression list maintained and applied across all CRM channels.
- Annual RG training for all staff and for affiliates with player-facing creative.

Review cycle: Annually, plus interim updates following regulator guidance.

POL-4.04 — Complaints Handling and Alternative Dispute Resolution

Purpose: Resolve player complaints fairly, transparently and within defined service levels, and provide a clear path to independent dispute resolution.

Scope: All player complaints, irrespective of channel.

Policy owner: Complaints Officer.

Key principles:

- Complaints are welcomed as a source of learning.
- Players have a right to a clear, written final response.
- Independent dispute resolution is available free of charge to the player at the Level-3 stage.

Key controls:

- Two internal levels of review (front-line and Complaints Officer) before final response.
- Maximum 8 weeks from receipt to final response.
- Complaints register and monthly trend reporting to the Compliance & Risk Committee.

Review cycle: Annually.

POL-4.05 — Bonus, Promotions and Marketing

Purpose: Ensure promotions are clear, fair and not misleading, comply with applicable laws and licence conditions, and do not target vulnerable groups.

Scope: All promotions, bonus campaigns and marketing communications including affiliate creatives.

Policy owner: Head of CRM (ServHGR) with Compliance Officer sign-off.

Key principles:

- Promotional terms are written in plain language and are accessible before opt-in.
- Significant terms (wagering, max bet, eligible games, expiry) are not buried in the small print.
- No targeting of self-excluded, excluded or RG-flagged players.
- No targeting of minors or restricted markets.
- All claims are accurate and substantiated.

Key controls:

- Pre-launch compliance review of every campaign and creative.
- Affiliate creative approval gate.
- Suppression of excluded players from every CRM segment.
- Periodic review of historical campaigns for fairness and outcomes.

Review cycle: Annually.

POL-4.06 — Data Protection and Privacy

Purpose: Protect the personal data of players, employees and other data subjects in line with the Curaçao data protection ordinance and, where applicable, the GDPR.

Scope: All processing of personal data by Purple Bay B.V. and its processors (including ServHGR Ltd).

Policy owner: Data Protection Officer (DPO).

Key principles:

- Lawfulness, fairness and transparency.
- Purpose limitation and data minimisation.
- Accuracy, storage limitation and integrity.
- Accountability — records of processing, DPIAs where required, and demonstrable compliance.

Key controls:

- Public privacy notice covering categories of data, purposes, legal bases, sharing, retention and rights.
- Records of Processing Activities (RoPA) maintained by the DPO.
- Data Processing Agreements with every processor, including ServHGR Ltd and PSPs.
- Subject access, rectification, erasure and portability request workflow with statutory deadlines.
- Data breach response procedure with notification to the supervisory authority within the statutory window where applicable.

Review cycle: Annually.

POL-4.07 — Information Security

Purpose: Protect the confidentiality, integrity and availability of the Company's information assets, players' data and gaming operations against accidental and deliberate threats.

Scope: All Purple Bay B.V and ServHGR Ltd personnel, contractors, systems, networks and information assets.

Policy owner: CTO Consultant (with support from the Information Security function).

Key principles:

- Risk-based control selection aligned with ISO/IEC 27001 control objectives.
- Defence in depth: prevention, detection and response.
- Least privilege and need-to-know access.
- Security by design and by default in all change activity.

Key controls:

- Network segregation, hardened images, end-point protection and centralised logging.
- Multi-factor authentication for all administrative access and for all access to player data.
- Vulnerability management with monthly internal scans and at least annual independent penetration testing.
- Encryption of personal and financial data at rest and in transit.
- Security awareness training, phishing simulation and just-in-time access reviews.

Review cycle: Annually.

POL-4.08 — Business Continuity and Disaster Recovery

Purpose: Ensure that the Company can continue critical operations during disruptive events and recover its services within agreed objectives.

Scope: All critical business processes and supporting technology, including those delivered by ServHGR Ltd and third parties.

Policy owner: CTO Consultant.

Key principles:

- Critical services are identified through a business impact analysis.
- Recovery time and point objectives are defined and tested.
- Plans are exercised at least annually and after material change.

Key controls:

- Documented BC/DR plan covering technology, people, premises and suppliers.
- Hot-warm architecture for the gaming platform with geographically separated infrastructure.
- At least annual DR test and lessons-learned process.
- Vendor BC/DR review for critical suppliers (PSP, KYC, hosting, game studios).

Review cycle: Annually.

POL-4.09 — Player Funds Protection

Purpose: Ensure that funds owed to players are at all times available to them and are not used by the Company as working capital or to meet other liabilities.

Scope: All player deposit balances and balances arising from winnings.

Policy owner: CEO with Finance.

Key principles:

- Player funds are recognised as a separate liability in the ledger.
- Player funds are held in a designated safeguarded account at a regulated financial institution, separate from operating accounts.
- The safeguarded balance is reconciled daily against the aggregate player liability.

Key controls:

- Daily reconciliation under SOP-3.12.
- Independent verification of the safeguarded balance by the external auditor at least annually.
- No use of player funds for any non-player-facing payment.

Review cycle: Annually.

POL-4.10 — Game Fairness and Random Number Generation

Purpose: Ensure that all games offered are fair, that the published return-to-player (RTP) reflects the certified RTP, and that the random number generator (RNG) underpinning gameplay is independently tested.

Scope: All games offered through the Company's platform.

Policy owner: CTO Consultant with Compliance Officer.

Key principles:

- Only games supplied by studios with valid third-party RNG/RTP certification are offered.
- Certificates are tracked centrally and removed games are flagged before expiry.
- Player-facing odds, paytables and RTP are accurate at all times.

Key controls:

- Game catalogue register with certificate references and expiry dates.
- Quarterly review of certificate expiries.
- Pause/withdrawal procedure for games with disputed integrity.

Review cycle: Annually.

POL-4.11 — Outsourcing

Purpose: Govern the use of third parties, particularly ServHGR Ltd, in the delivery of regulated activities, so that Purple Bay B.V maintains full control, oversight and accountability.

Scope: All outsourcing arrangements, with particular attention to intragroup outsourcing to HGR Services.

Policy owner: Compliance Officer.

Key principles:

- Outsourcing does not transfer regulatory accountability.
- Critical or important functions require Board approval before outsourcing.
- Outsourced functions are subject to the same standards and oversight as if performed internally.
- Concentration risk and group conflict of interest are explicitly managed.

Key controls:

- Written MSA with ServHGR Ltd covering service description, SLA, audit rights, sub-outsourcing, data protection, BC/DR, termination and exit planning.
- Quarterly oversight reporting from ServHGR Ltd to the Compliance Officer.
- Annual outsourcing risk assessment to the Board.
- Documented exit plan capable of execution within an agreed period.

Review cycle: Annually.

POL-4.12 — Conflicts of Interest

Purpose: Identify, prevent or manage actual, potential and perceived conflicts of interest, including those arising from common ownership across the PPB group.

Scope: All directors, officers, employees, consultants and outsourced personnel.

Policy owner: Compliance Officer.

Key principles:

- Conflicts are disclosed and recorded.
- Conflicted persons do not participate in the decision concerning the conflict.
- Intragroup transactions are conducted on arm's-length terms.

Key controls:

- Annual conflicts declaration for all relevant persons.
- Conflicts register maintained by the Compliance Officer.
- Intragroup transactions reviewed and benchmarked annually.

Review cycle: Annually.

POL-4.13 — Sanctions

Purpose: Prevent dealings with persons and jurisdictions subject to international sanctions and ensure full compliance with applicable sanctions regimes.

Scope: All players, suppliers, counterparties and employees.

Policy owner: Compliance Officer.

Key principles:

- Zero tolerance for breaches.
- Multi-list screening: UN, EU, OFAC, UK and locally implemented sanctions.
- Sanctions risk is assessed at onboarding and continuously thereafter.

Key controls:

- Daily delta screening (SOP-3.14).
- Immediate freeze of accounts on confirmed hit.
- Annual sanctions training for relevant staff.

Review cycle: Annually.

POL-4.14 — Affiliate Standards

Purpose: Ensure that affiliates promote the Company's products in a compliant, accurate and responsible manner.

Scope: All affiliates and the Company's affiliate programme.

Policy owner: Head of CRM (HGR) with Compliance Officer sign-off.

Key principles:

- Affiliates must conduct themselves to the same standards as the Company.

- Affiliates targeting minors, restricted markets or vulnerable groups are terminated.
- Affiliate creative must be pre-approved before use.

Key controls:

- Affiliate due diligence at onboarding and at material change.
- Creative approval gate.
- Daily traffic and quality review (SOP-3.11).
- Termination clauses for breach.

Review cycle: Annually.

POL-4.15 — Workplace Conduct, Health and Safety

Purpose: Provide a safe, respectful and inclusive workplace and promote the well-being of staff.

Scope: All Purple Bay B.V. personnel and consultants; ServHGR Ltd personnel are bound by the equivalent ServHGR Ltd policy.

Policy owner: CEO.

Key principles:

- Zero tolerance for harassment, bullying or discrimination.
- Compliance with applicable employment, health and safety law.
- Well-being and reasonable work patterns are actively supported.

Key controls:

- Code of Conduct acknowledged annually.
- Confidential reporting channel and Whistleblowing Policy (POL-4.16).
- Annual workplace risk assessment.

Review cycle: Annually.

POL-4.16 — Whistleblowing

Purpose: Encourage and protect the reporting of suspected wrongdoing.

Scope: All persons working for or with the Company.

Policy owner: Compliance Officer (with route to the Chair of the Board).

Key principles:

- Reports may be made in confidence and, where permitted, anonymously.
- No detriment for good-faith reporting.
- Reports are investigated promptly and proportionately.

Key controls:

- Whistleblowing email and mailbox monitored by the Compliance Officer.
- Alternative route directly to the Chair where the report concerns a member of management.
- Annual reminder communication and training reference.

Review cycle: Annually.

POL-4.17 — Record Retention

Purpose: Retain records for the periods required by applicable law and licence conditions and dispose of them securely thereafter.

Scope: All Company records, regardless of medium.

Policy owner: Compliance Officer with DPO.

Key principles:

- Retention periods are documented in the Retention Schedule.
- Personal data is not retained beyond what is necessary.
- Records relevant to AML/CFT are retained for at least ten (10) years from the end of the relationship.

Key controls:

- Retention schedule reviewed annually.
- Secure destruction process for paper and electronic records.
- Legal hold process where records are subject to investigation or dispute.

Review cycle: Annually.

5. Quality, Control and Assurance Framework

5.1 Internal control statement

The Board confirms its responsibility for the system of internal controls and for reviewing its effectiveness. The system is designed to manage rather than eliminate risk; it cannot provide absolute assurance against material misstatement or loss.

5.2 Key risk indicators (KRIs)

Indicator	Owner	Threshold	Reporting cadence
Unverified accounts > 7 days	Compliance Officer	< 1% of active base	Weekly
AML alerts aged > 2 business days	MLRO	0	Daily
Self-exclusion processing time	RG Officer	100% within 1 hour	Daily
Complaints aged > 8 weeks	Complaints Officer	0	Weekly
Chargeback rate (value)	Head of Payments	< 0.5%	Weekly
Platform uptime (rolling 30d)	CTO Consultant	≥ 99.9%	Daily
Player-funds variance	Finance	0	Daily
Sanctions hits unresolved > 24h	Compliance Officer	0	Daily

5.3 Internal audit

Internal audit is outsourced to Xecutive Corporate Management B.V. and operates under a charter approved by the Board. An annual audit plan covers, on a multi-year basis: AML/CFT, KYC, responsible gambling, complaints, outsourcing oversight, payments, information security, business continuity and player funds. Findings are reported to the Compliance & Risk Committee and the Board.

5.4 Independent third-party testing

Independent testing of gaming systems and RNG is performed by each game provider adhering to the regulations. Penetration testing is performed normally on at least an annual basis and after material change.

5.5 Continuous improvement

Findings from audits, regulator interactions, complaints, RG cases and incidents feed a single Improvement Backlog managed by the Compliance Officer. Items are prioritised by risk and customer impact, and progress is reported monthly.

6. Safety and Player Protection

Player safety is treated as a first-order objective, on equal footing with commercial and operational goals. This Section sets out the principal measures the Company takes.

6.1 Underage gambling prevention

- Minimum age 18 enforced at registration via documentary identity verification.
- Any account suspected to belong to a minor is suspended immediately, investigated, and closed if confirmed.
- Funds in an underage account are returned to the source of funds; winnings are forfeit.
- Marketing creatives must not appeal to or be placed where they are likely to be seen primarily by minors.

6.2 Self-exclusion

- Self-exclusion can be requested via any player-facing channel and takes effect within 1 hour of receipt.
- Minimum self-exclusion period: 6 months; longer periods available; permanent exclusion is supported.
- Self-excluded players are removed from all marketing segments and cannot register a new account during the exclusion period.
- Where a national self-exclusion register exists in a market the Company serves and integration is required by licence, the Company integrates and checks it before account opening and deposit.

6.3 Player-imposed limits and reality checks

- Deposit, loss, wager and session-time limits are available to every player and applied immediately when set or decreased.
- Limit increases are subject to a cooling-off period before they take effect.
- Reality checks display elapsed session time and net position at configurable intervals.

6.4 Identifying and supporting at-risk players

- A behavioural model identifies risk markers (chasing losses, late-night activity spikes, sudden increases in stake or session length, repeated cancelled withdrawals, etc.).
- Flagged players are contacted by the RG team, offered RG tools and signposted to professional help services.
- Where appropriate, protective limits or temporary suspensions are imposed.

6.5 Marketing safeguards

- Suppression list of self-excluded and RG-flagged players is applied to every CRM segment before send.
- Affiliate creatives are pre-approved and audited.

- Bonus offers and reactivation campaigns are not sent to excluded players under any circumstances.

7. Contact Information

7.1 Internal contacts — Purple Bay B.V.

Role	Name	Email	Notes
Chief Executive Officer	Alexandre Etienne Assouline	admin@purplepaybv.com	Ultimate accountability
CTO Consultant	Alexandre Etienne Assouline	admin@purplepaybv.com	Technology, security, BC/DR
Compliance Officer	Stacey-Lee Portillo	sportillo@xcm.cw	Owner of this Manual
Money Laundering Reporting Officer (MLRO)	Everhona Makaya	emakaya@xcm.cw	SAR/STR filings
Data Protection Officer (DPO)	Stacey-Lee Portillo	sportillo@xcm.cw	Privacy and data subject rights
Responsible Gambling Officer	Pierre Flermoen	risk@purplebaybv.com	RG cases and self-exclusion
Curaçao Local Representative / Key Person	Stacey-Lee Portillo	sportillo@xcm.cw	Liaison with CGA
Complaints Officer	Stacey-Lee Portillo	sportillo@xcm.cw	Level-2 complaints handling

7.2 Regulator

Authority	Detail
Name	Curaçao Gaming Authority (CGA)
Address	Korporaalweg 10, Willemstad, Curaçao
Email (general)	info@gamingauthority.cw
Website	https://gamingauthority.cw
Company licence number	OGL/2024/1368/0895

7.3 Alternative Dispute Resolution (ADR) for players

Players who are not satisfied with the Company's final response to their complaint are entitled to refer the matter, free of charge, to the Company's designated Alternative Dispute Resolution provider. The ADR provider is independent of the Company and its decision is binding on the Company.

7.4 Financial Intelligence Unit

In Curaçao, unusual transactions are reported to the Meldpunt Ongebruikelijke Transacties (FIU Curaçao) under the LMOT. The MLRO is the sole point of contact between the Company and the FIU.

Field	Detail
Authority	FIU Curaçao (Meldpunt Ongebruikelijke Transacties)
Website	https://www.fiucuracao.cw
Contact	Via the prescribed reporting channel only; the MLRO maintains the contact details.

7.6 Key external service providers

Function	Provider	Notes
KYC / identity verification	Dilisense	DPA in place
Payments orchestration	PaymentIQ (PIQ)	Multi-PSP routing
Game studios / aggregators	Per integration register	Each holds independent RNG/RTP certification
Affiliate platform	MyAffiliates	Tracking, attribution and payouts
Financial reconciliation	Finera	Reconciliation tooling
Internal audit	Xecutive Corporate Management B.V.	

Annex A — Glossary

Term	Meaning
ADR	Alternative Dispute Resolution
AML / CFT	Anti-Money Laundering / Counter-Terrorist Financing
BC/DR	Business Continuity / Disaster Recovery
CDD / SDD / EDD	Customer / Simplified / Enhanced Due Diligence
CGA	Curaçao Gaming Authority
CRM	Customer Relationship Management
DPA	Data Processing Agreement
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
FIU	Financial Intelligence Unit
GGR / NGR	Gross / Net Gaming Revenue
KRI / KPI	Key Risk Indicator / Key Performance Indicator
KYC	Know Your Customer
LID	Landsverordening Identificatie bij Dienstverlening
LMOT	Landsverordening Melding Ongebruikelijke Transacties
LOK	Landsverordening op de Kansspelen
MLRO	Money Laundering Reporting Officer
MSA	Master Services Agreement
PEP	Politically Exposed Person
PSP	Payment Service Provider
RG	Responsible Gambling
RNG / RTP	Random Number Generator / Return To Player
SAR / STR	Suspicious Activity / Transaction Report
UBO	Ultimate Beneficial Owner

Annex B — Document Review Log

Section	Last reviewed	Next review	Reviewer
1. Company Overview	05/01/2026	05/01/2027	Compliance Officer
2. Governance and Organisation	05/01/2026	05/01/2027	Compliance Officer
3. Daily Operational Processes	05/01/2026	05/01/2027	Compliance Officer / HGR COO
4. Policies and Guidelines	12/01/2026	12/01/2027	Compliance Officer
5. Quality, Control and Assurance	12/01/2026	12/01/2027	Compliance Officer
6. Safety and Player Protection	12/01/2026	12/01/2027	RG Officer
7. Contact Information	05/01/2026	Quarterly	Compliance Officer

Annex C — Restricted and Prohibited Territories

The Company does not knowingly accept players resident in the territories listed below. The list is reviewed at least quarterly.

Afghanistan, Albania, Algeria, Angola, Austria, Bahrain, Canada, China, Cuba, Czech Republic, Dutch Kingdom, Eritrea, Estonia, Ethiopia, Finland, Georgia, Greece, Greenland, Hong Kong, Indonesia, Jordan, Iran, Iraq, Ireland, Italy, Kuwait, Libya, Lithuania, Malaysia, Malta, Mauritania, Mauritius, Morocco, Norfolk Island, Norway, N. Korea, Oman, Pakistan, Portugal, Qatar, Rwanda, Saudi Arabia, Slovenia, Somalia, South Sudan, Spain, Sudan, Syria, Turkey, Tunisia, UAE, Yemen, United States and its dependencies, military bases and territories including but not limited to Am. Samoa, Guam, Marshall Islands, N. Mariana Islands, Puerto Rico, and Virgin Islands.

Annex D — Reference List of Laws and Regulations

- Landsverordening op de Kansspelen (LOK) and subsidiary regulations and directives issued by the CGA.
- Landsverordening Identificatie bij Dienstverlening (LID).
- Landsverordening Melding Ongebruikelijke Transacties (LMOT).
- National Ordinance on the Penalisation of Money Laundering and Terrorist Financing.
- National Ordinance on the Protection of Personal Data; and, where applicable, Regulation (EU) 2016/679 (GDPR).
- National Ordinance on UBO Registration.
- Applicable economic sanctions regimes (UN, EU, OFAC, UK, locally implemented).