

Neptune Projects SRL

Operating brands: casiny.com · vegastars.com · voltrush.com · royalerush.com

Tobique B2C Gaming Licence

Compliance Policy Suite

KYC · CDD · EDD · Transaction Monitoring
Payment Methods · PEP & Sanctions Screening

Field	Value
Version	1
Date of issue	April 2026
Document owner	Arvids Vitolins - AML Officer / MLRO
Approved by	Board of Directors
Regulatory framework	Tobique B2C Gaming Licence - Tobique Gaming Act 2023, AML Regulations & AML Code of Practice
Brands in scope	casiny.com · vegastars.com · voltrush.com · royalerush.com
Next review date	April 2027 (annual)
Classification	Confidential - Internal Use Only

Version Control

Version	Date	Author	Description
1.0	April 2026	Arvids Vitolins - AML Officer	Initial document - created as part of the Company Compliance Programme.

1. Purpose and Scope

This document is the Compliance Policy Suite for Neptune Projects SRL (the "Company"). It sets out in a single reference document the obligations and procedures governing Know Your Customer (KYC), Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Transaction Monitoring, Payment Methods, and PEP & Sanctions Screening.

This Policy applies to:

- Neptune Projects SRL and all its officers, directors, and employees;
- All brands operated under the Company's licence: casinyl.com · vegastars.com · voltrush.com · royalerush.com;
- All subsidiary payment agent entities in scope (see Annex A); and
- All third-party service providers acting on behalf of the Company to the extent required by applicable law.

This Policy must be read in conjunction with the Company's AML/CFT Policy, the Responsible Gambling Policy, the Business Risk Assessment, and all other policies referenced herein.

2. Regulatory Framework

The Company holds the following licence and is subject to the requirements set out below:

Licence Type	Issuing Authority	Licence Number
Tobique B2C Gaming Licence	First Nations of Tobique - Tobique Gaming Commission	0000020

The following instruments form the primary regulatory framework for this Policy:

- Tobique Gaming Act 2023 (the "Gaming Act");
- Regulations Concerning Anti-Money Laundering and Counter-Terrorist Financing (the "AML Regulations") - enacted pursuant to section 22 of the Gaming Act;
- AML/CTF Code of Practice (the "AML Code") - to be read in conjunction with the AML Regulations;
- General Code of Practice for Remote Gaming License Holders (the "General Code"); and
- FATF 40 Recommendations - applied as the international standard for AML/CFT compliance.

In any conflict between the AML Regulations and the AML Code of Practice, the AML Regulations shall prevail.

3. Key Definitions

Term	Definition
BRA	Business Risk Assessment - a documented assessment of the ML/TF/PF risks the Company is exposed to, prepared per AML Regulations Section 9 and AML Code of Practice Section 10.
CDD	Customer Due Diligence - the process of identifying and verifying a customer's identity and assessing the risk they pose.
CVC	Convertible Virtual Currency - any crypto or stablecoin accepted by the Company as a deposit or withdrawal method.
EDD	Enhanced Due Diligence - additional checks applied to higher-risk customers, PEPs, or transactions above defined thresholds.

Term	Definition
FIU	Tobique Financial Intelligence Unit - the recipient of external Suspicious Activity Reports.
KYC	Know Your Customer - the set of identity verification processes applied at onboarding.
ML/TF/PF	Money Laundering, Terrorist Financing, and Proliferation Financing.
MLRO	Money Laundering Reporting Officer - the designated officer responsible for receiving internal SARs and filing external disclosures with the FIU.
PEP	Politically Exposed Person - an individual who holds or has held a prominent public function.
Pre-paid card	A payment card not linked to a personal bank account or verified identity - considered a high-risk anonymous payment instrument.
RG	Responsible Gambling - the framework of customer protection measures under the General Code of Practice Sections 17–19.
SAR	Suspicious Activity Report - an internal or external report of suspected ML/TF/PF activity.
SDD	Simplified Due Diligence - reduced CDD measures applicable to demonstrably low-risk customers only.
Source of funds	The origin of the specific funds being deposited or used in a transaction.
Source of wealth	The totality of a customer's economic activity and the means by which they accumulated their assets.
SumSub	The Company's contracted third-party KYC provider - the sole approved identity verification platform.
TGC	Tobique Gaming Commission - the regulator issuing the Company's gaming licence.

4. Roles and Responsibilities

4.1 Board of Directors

The Board is responsible for approving this Policy and overseeing its implementation. The Board reviews all compliance policies at least annually.

4.2 AML Officer / MLRO

The AML Officer for Neptune Projects SRL is Arvids Vitolins. The AML Officer is responsible for:

- Day-to-day implementation and oversight of this Policy;
- Receiving, reviewing, and determining the outcome of all internal SARs within 5 business days;
- Filing external SARs with the Tobique FIU where required;
- Approving all EDD assessments and High-risk customer relationships;
- Reviewing all PEP relationship decisions;
- Quarterly AML/CFT effectiveness reporting to the Board; and
- Ensuring all staff complete AML/CFT training annually.

The AML Officer contact for this entity is: Arvids Vitolins. All internal SARs and EDD referrals must be directed to this officer.

4.3 Payments & Fraud Team

The Payments & Fraud Team is responsible for:

- Daily deposit and withdrawal checks against the monitoring rules in Section 7;
- Flagging suspicious payment activity to the AML Officer within 24 hours of identification;
- Enforcing closed-loop refund and payment method controls; and
- Maintaining transaction records in a format accessible for regulatory inspection.

4.4 Responsible Gaming Manager

The Responsible Gaming Manager (designated under General Code of Practice Section 17.7) coordinates with the AML Officer on all touchpoints between Responsible Gambling and AML/CFT controls (see Section 11).

4.5 All Staff

All staff must complete annual AML/CFT training, report suspicions to the AML Officer without delay, and never tip off a subject under investigation.

5. Customer Due Diligence (CDD)

MANDATORY: SumSub is the sole approved KYC provider for ALL brands operated by Neptune Projects SRL - casiny.com · vegastars.com · voltrush.com · royalerush.com. No customer may complete a coin purchase, deposit, or withdrawal on any brand without first completing SumSub verification. Ad-hoc or manual-only verification is not acceptable and does not satisfy this Policy.

5.1 When CDD is Required

CDD must be completed before the EARLIER of:

- 30 days from the customer's registration;
- The customer's cumulative deposits reaching €2,000; or
- The customer's first withdrawal request.

(Per TGC General Code of Practice, Section 6.1 - whichever event occurs first.)

In addition, CDD-related actions must be triggered on the following events:

- A customer completes registration on any brand;
- A customer makes their first coin purchase or deposit on any brand;
- A customer's cumulative deposits reach €2,000 (operational risk-labelling trigger);
- A material change occurs in the customer's account behaviour, payment method, or risk profile.

No deposit or withdrawal may be processed until the customer's SumSub verification is complete and the result is passed to the Company's back-office.

5.2 Standard CDD - Information Required

Information Required	Verification Method
Full legal name	Government-issued photo ID (passport, national ID, driving licence) via SumSub

Information Required	Verification Method
Date of birth - must be 18 or over	SumSub identity check - age verification configured for 18+ only
Country of residence	ID document + IP address cross-check via SumSub
Email address	Email verification at registration
Electronic footprint (IP, device ID, browser cookies)	Captured automatically at registration - per Tobique General Code s.5.3
Payment method details	Card BIN/last-4, wallet address, or bank account captured via PSP at first deposit

5.3 Third-Party KYC Provider - SumSub

SumSub is the sole contracted KYC provider. SumSub must be active and processing verifications for every brand before any brand accepts deposits. The following requirements apply:

- A current Data Processing Agreement (DPA) must be in place between the Company and SumSub at all times;
- SumSub settings must be configured to block all customers under 18;
- SumSub liveness checks must be enabled for all brands;
- PEP and sanctions screening within SumSub must be set to automated, not case-by-case (see Section 9); and
- The AML Officer must conduct a quality review of SumSub output at least annually.

No other third-party tool (including CRM or marketing platforms) may be used to collect, store, or process customer identity data for CDD purposes without prior written approval from the AML Officer and a DPA in place.

5.4 Simplified Due Diligence (SDD)

SDD may only be applied where the AML Officer has documented the rationale and confirmed in writing that the customer presents demonstrably low risk. SDD does not exempt a customer from any monitoring obligations.

5.5 Ongoing Monitoring

Once a customer is onboarded, the Company monitors the customer relationship on an ongoing basis to ensure activity is consistent with the declared customer profile. Ongoing monitoring includes:

- Daily deposit and withdrawal checks (see Section 7);
- Periodic review of risk labels - triggered by changes in deposit pattern, withdrawal method, or fraud flags;
- Annual re-verification for High-risk customers; and
- Immediate re-verification on any change of payment method or significant increase in deposit volume.

5.6 Age Verification

Age Verification is mandatory and must be completed before the EARLIER of:

- 48 hours from the customer's registration; or
- The customer's cumulative deposits reaching €500.

(Per TGC General Code of Practice, Section 21.5 - whichever event occurs first.)

Where age verification is not completed within this window, the account must be:

- Supervised pending verification;
- Reviewed by the Payments & Fraud Team and AML Officer;
- Restricted or suspended in line with GCoP 21.5 if age cannot be confirmed.

During the age verification period:

- Customers may be permitted to deposit funds and participate in gaming; however
- No withdrawal of any deposit or winnings may be processed until age has been formally verified, irrespective of the broader CDD status.

Where the customer is subsequently confirmed as under 18:

- The account must be suspended immediately;
- Deposits must be returned to the customer (no winnings paid);
- Any winnings to be paid in respect of such gaming must be forfeited to the Tobique Gaming Commission per GCoP 21.7;
- The case must be reported to the Commission per GCoP 20.1; and
- The Responsible Gaming Manager must be notified.

Age verification is performed via SumSub at registration and continually monitored through the SumSub configuration that blocks all customers under 18. Records of age verification (including any failed attempts) are retained per Section 12 of this Policy.

6. Enhanced Due Diligence (EDD)

EDD is mandatory and non-negotiable. Any customer meeting one or more of the EDD triggers below must not be permitted to continue transacting until EDD is completed and approved by the AML Officer. There are no exceptions to this rule.

6.1 EDD Triggers - Automatic

EDD must be initiated automatically when any of the following conditions are met:

#	Trigger Condition	Action Required
1	Customer's cumulative deposits reach or exceed €5,000 within any rolling 30-day period	Initiate EDD within 24 hours. Suspend further deposits until EDD complete.
2	Customer's risk label is set to High in the back-office	Initiate EDD within 24 hours of label change.
3	Customer is identified as a PEP at any point	Freeze account immediately. MLRO review within 48 hours.
4	Sanctions match identified via SumSub screening	Freeze account immediately. Refer to Legal and FIU.
5	Suspicious activity alert raised by Payments & Fraud Team	MLRO to review internal SAR within 5 business days.
6	Customer requests a refund to a different payment method than used for deposit	Flag for EDD review before any refund is processed.
7	Customer uses a crypto wallet flagged by blockchain analytics	Freeze pending MLRO review.

6.2 EDD Measures

EDD must include, but is not limited to, the following measures applied in proportion to the risk presented:

- Collection and verification of source of funds documentation - bank statements, payslip, proof of business income, or equivalent;
- Collection of source of wealth information where cumulative deposits exceed €5,000 in any 12-month period;
- Enhanced adverse media search - Google search plus third-party screening tool - documented in the customer file;
- Review of all previous transactions to identify consistency with the declared profile;
- Increased monitoring frequency - weekly review of all transactions for High-risk customers;
- For PEPs specifically: confirmation of current role, confirmation of legitimate source of income, and senior management approval; and
- Written sign-off by the AML Officer confirming whether the relationship may continue.

6.3 EDD Process and SLA

The EDD process follows these steps in order:

- Trigger detected - automated system or Payments & Fraud Team raises flag.
- Account suspended from deposits and withdrawals pending EDD completion.
- AML Officer notified within 24 hours of trigger.
- EDD questionnaire sent to customer within 48 hours of trigger.
- Customer has 10 business days to provide required documentation.
- AML Officer reviews documentation and completes EDD checklist (see Annex D).
- AML Officer decision within 5 business days of receiving complete documentation: (a) account reinstated with enhanced monitoring, (b) account closed, or (c) SAR filed with FIU.
- Outcome documented in customer file and retained for minimum 5 years.

6.4 Failure to Complete EDD

If a customer fails to provide required EDD documentation within 10 business days, the account must be permanently closed and a SAR must be considered. The AML Officer must document the decision in all cases.

7. Transaction Monitoring

7.1 Monitoring Framework

Transaction monitoring is conducted through a combination of automated back-office rules and daily manual reviews by the Payments & Fraud Team. The objective is to detect activity inconsistent with the customer's declared profile or presenting indicators of ML/TF.

The following monitoring activities are mandatory:

Activity	Description	Frequency
Deposit checks	Review all deposits flagged by automated rules. Check for structuring (multiple deposits just below thresholds), unusual originating countries, and new payment methods.	Daily
Withdrawal checks	Review all withdrawals above €500 or flagged by automated rules. Verify withdrawal method matches deposit method for all non-bank-transfer withdrawals.	Daily

Activity	Description	Frequency
High-risk customer review	Full review of all transactions for customers labelled High risk.	Weekly
Big winners procedure	Enhanced review for any single withdrawal request above €5,000 - verify source of funds if not already on file.	On event
30-day cumulative monitoring	Automated flag when any customer's cumulative deposits reach €2,000 (warning) or €5,000 (EDD trigger).	Real-time
Cross-payment-method aggregation	Total deposits across all payment methods counted together for threshold purposes - not per instrument.	Real-time
Crypto wallet screening	All crypto deposit wallets screened via blockchain analytics tool before funds accepted.	Per transaction

7.2 Red Flags - Online Gaming Specific

The following behaviours are casino-specific red flags drawn from the Tobique AML Code of Practice and FATF guidance. Each must be reviewed by the Payments & Fraud Team and escalated to the AML Officer where two or more are present simultaneously:

- Rapid deposit and withdrawal with minimal or no gaming activity - funds deposited and withdrawn within 24 hours with less than 10% wagered;
- Refund requests to a different payment method or bank account than used for the original deposit;
- Multiple accounts linked to the same device fingerprint, IP address, or payment instrument;
- Deposits significantly exceeding the customer's stated income or prior spending patterns;
- Use of VPN, proxy, or IP address inconsistent with the customer's registered country;
- Pre-paid card deposits followed by requests to withdraw via bank transfer;
- CVC deposits from wallets associated with mixing services, dark web markets, or flagged by blockchain analytics;
- Customers excluded for responsible gambling reasons who re-register or attempt to circumvent exclusion controls (see Section 11);
- Split deposits across multiple payment methods to remain below monitoring thresholds;
- Customers reluctant to provide verification documentation when requested; and
- Requests to change withdrawal details shortly before or after a large deposit.

7.3 Automated Rule Engine

The following automated rules must be implemented in the back-office system and reviewed monthly for effectiveness:

Rule	Threshold	Automated Action
Cumulative deposit - 30 days	€2,000 in 30 days	Warning flag - assign risk label Medium
Cumulative deposit - 30 days	€5,000 in 30 days	EDD trigger - suspend new deposits
Single deposit	€1,000 from pre-paid card	Automatic High-risk label + EDD trigger
Withdrawal-to-deposit ratio	Less than 10% wagered	Flag for suspicious activity review
Same device / IP - multiple accounts	2 or more accounts	Suspend both pending review

Rule	Threshold	Automated Action
Cross-currency transfer	Any Fiat - Crypto or Crypto-Fiat	Manual review required before processing
Crypto wallet risk score	High-risk wallet identified by analytics	Block transaction - refer to AML Officer

8. Payment Methods Policy

Pre-paid card acceptance creates an anonymous payment instrument risk. Pre-paid cards are restricted under this Policy - see Section 8.3. Cross-currency transfers are restricted under Section 8.5.

8.1 Accepted Payment Methods

The Company accepts the following payment methods, subject to the restrictions in this section:

Payment Method	Conditions	Max per Customer	Risk Level
Debit or credit card (personal)	Must be in the customer's verified name. BIN and last-4 digits recorded.	2 cards	Standard
Bank transfer	Must originate from a bank account in the customer's verified name.	1 account	Standard
Stablecoin (e.g. USDT, USDC)	Wallet must pass blockchain analytics screening. Withdrawal to originating wallet only.	1 wallet	Elevated
Cryptocurrency (non-stablecoin)	Only high market cap cryptocurrency is allowed.	1 wallet	Elevated

8.2 Maximum Payment Methods per Customer

No customer may have more than three (3) active payment methods registered on their account at any one time. This limit applies across all brands operated by the Company - a customer registered on multiple Neptune brands (Casiny, Vegastars, Voltrush, RoyaleRush) is subject to the same three-method limit in aggregate.

Adding a new payment method beyond the limit requires removal of an existing method and written confirmation from the customer that the new method is in their name.

8.3 Pre-paid Card Restrictions

Pre-paid cards are anonymous payment instruments that present a material ML/TF risk. The Company does not accept pre-paid cards as a standard deposit method. The following restrictions apply:

- Pre-paid card deposits are capped at €50 per single transaction;
- Any customer depositing via pre-paid card is automatically assigned a High risk label;
- Pre-paid card customers must complete EDD (Section 6) before any withdrawal is processed;

- Pre-paid card refunds may only be made to the exact card used for the original deposit - no cross-method refunds;
- The AML Officer must review all pre-paid card refund requests above €20 before approval; and
- The Company will eliminate pre-paid card acceptance entirely as a medium-term objective - target date to be set by the Board.

8.4 Closed-Loop Refund Rule

The Company enforces a strict closed-loop refund policy:

- All refunds must be returned to the exact payment method and account or wallet used for the original deposit;
- Under no circumstances may a refund be issued to a different card, bank account, or wallet than the one used to deposit, except where the original method is demonstrably closed and no longer available;
- Any request for a refund to a different method must be reviewed by the AML Officer and treated as a potential ML/TF red flag;
- The maximum number of refunds a customer may request in any 30-day period is three (3) - further requests require AML Officer approval; and
- All refund requests and approvals must be documented and retained for 5 years.

8.5 Cross-Currency Transfers (Fiat-to-Crypto / Crypto-to-Fiat)

Cross-currency transfers between fiat and crypto payment methods present a significant ML/TF risk by enabling source-of-funds obscurity. The following restrictions apply:

- A customer who has deposited via a fiat method (card or bank transfer) may not withdraw via crypto, and vice versa;
- Cross-currency transfers are prohibited unless the customer has completed EDD and the AML Officer has approved the transfer in writing; and
- Any system capability that allows cross-currency transfers must have an automated block applied pending AML Officer approval.

8.6 Crypto / CVC Controls

For customers transacting via stablecoin or CVC:

- All deposit wallets must be screened via the Company's blockchain analytics tool before funds are accepted;
- Wallets with a risk score of High or flagged for association with mixing services, dark web activity, or sanctions must be rejected and the customer flagged for the AML Officer;
- Wallet ownership verification is required - the customer must confirm they control the wallet before a crypto withdrawal is processed; and
- Crypto withdrawals must go to the originating wallet address only - no new wallet destinations without re-verification.

9. PEP and Sanctions Screening

PEP and sanctions screening must be automated and applied to ALL customers at registration. Case-by-case screening is not compliant with the Tobique AML Code of Practice (section 20) and is not acceptable under this Policy.

9.1 Screening at Onboarding

All customers must be screened against PEP lists and applicable sanctions lists via SumSub's automated screening module at the point of registration, before any deposit or coin purchase is permitted.

SumSub must be configured to run automated screening - not case-by-case - against the following lists as a minimum:

- OFAC Specially Designated Nationals (SDN) list;
- United Nations Security Council Consolidated Sanctions List;
- European Union Consolidated Sanctions List;
- UK Office of Financial Sanctions Implementation (OFSI) list;
- HM Treasury Consolidated List; and
- Tobique Gaming Commission sanctions guidance where published.

9.2 Ongoing Screening

All active customers must be re-screened against the above sanctions lists on at least a monthly basis. Any new sanctions designation that matches an existing customer must be flagged to the AML Officer within 24 hours of the screening run.

9.3 PEP Identification and Procedure

When a customer is identified as a PEP at onboarding or during ongoing screening:

- Account is immediately suspended pending MLRO review;
- AML Officer must be notified within 24 hours;
- EDD is mandatory - additional ID, source of funds, source of wealth, and confirmation of current role required;
- AML Officer completes written risk assessment;
- Board approval required before relationship may be established or continued;
- PEP accounts are subject to enhanced transaction monitoring - reviewed weekly;
- PEP relationship reviewed every 6 months.

The Company considers PEPs to represent a higher inherent risk of bribery and corruption. The Company's default position is to decline PEP relationships unless the risk assessment demonstrates a clearly legitimate profile and source of funds.

9.4 Sanctions Match Procedure

When a customer matches a sanctions list entry:

- Account is frozen immediately - no deposits, withdrawals, or transfers may be processed;
- AML Officer and Legal team notified immediately;
- Funds on account are ring-fenced pending FIU guidance;
- SAR filed with Tobique FIU within the timeframe set out in Section 10.2;
- Account closed permanently;
- No communication with the customer that a sanctions match has been made - tipping-off prohibition applies.

9.5 Tipping-Off Prohibition

It is a criminal offence to disclose to any person that a SAR has been filed, that they are the subject of a sanctions or PEP investigation, or that a freeze has been imposed. Any staff member who discloses such information will face disciplinary action and may face criminal prosecution.

10. Suspicious Activity Reporting

10.1 Internal SARs

Any staff member who knows, suspects, or has reasonable grounds to suspect ML/TF/PF must submit an internal SAR to the AML Officer without delay using the form at Annex C. Do not act on the suspicion, do not tip off the customer, and do not discuss the matter with anyone other than the AML Officer.

The AML Officer must review every internal SAR within 5 business days and determine whether to file an external SAR with the Tobique FIU.

10.2 External SARs - Filing Timeline and FIU Registration

Neptune Projects SRL must be registered with the Tobique FIU in order to submit Suspicious Transaction Reports (STRs). Legal is responsible for confirming and documenting the FIU registration details. Until registration is confirmed, the AML Officer must consult Legal before taking any action on a potential SAR.

External SARs must be filed without delay, and in any case within five (5) working days of the MLRO determining that a credible suspicion exists.

The 'without delay' standard reflects the obligation under AML Regulations Section 25; the five-working-day ceiling is the operational maximum and is not a default. Where a credible suspicion is formed and the supporting analysis is straightforward, the SAR should be filed in materially less time than five working days. The MLRO must document, in every case, the date the suspicion was formed, the date the SAR was filed (or the decision not to file), and the rationale for the timeline taken.

11. RG / Compliance Touchpoints

This Policy operates in conjunction with the Company's Responsible Gambling Policy and procedures. The following touchpoints between AML/CTF and Responsible Gambling functions must be operationally maintained:

11.1 Self-Excluded Customer Detection

Where a customer attempts to re-register after a self-exclusion, or attempts to circumvent an active exclusion (a Section 7.2 red flag), the Payments & Fraud Team must:

- Block the registration or transaction immediately;
- Refer the case to the Responsible Gaming Manager within 24 hours;
- Refer the case to the AML Officer in parallel where the conduct also presents indicators of ML/TF (e.g., use of false identifying details, third-party payment methods);
- Document the case in the customer file and retain for the period set out in Section 12.

11.2 TGC Consolidated Self-Exclusion List Screening

All customers must be screened at registration against the Tobique Gaming Commission consolidated self-exclusion list (per General Code of Practice Section 19.11). The screening is performed alongside SumSub PEP/sanctions screening and is governed by this Policy and the Responsible Gambling Policy in combination.

Where a customer matches an entry on the TGC consolidated list:

- Registration must be refused or the account suspended where one already exists;
- The match must be referred to the Responsible Gaming Manager and the AML Officer;
- Any account balance must be remitted to the customer per the Responsible Gambling Policy.

11.3 EDD and RG Risk Indicators

Where EDD reveals customer behaviour consistent with problem gambling - including but not limited to deposit patterns inconsistent with declared income, attempts to bypass deposit limits, or withdrawal patterns suggesting chasing of losses - the AML Officer must refer the case to the Responsible Gaming Manager for parallel RG assessment. The AML decision and the RG decision are independent but coordinated.

11.4 Account Closure Coordination

Where an account is closed under this Policy (e.g., failed EDD, sanctions match, repeated SAR triggers), and the customer holds an account balance, the closure must be coordinated with:

- Finance / Payments - for balance remittance;
- The Responsible Gaming Manager - to ensure no parallel RG-driven action is in progress; and
- Customer Support - for customer communication consistent with tipping-off prohibitions.

11.5 SAR Cross-Reference with RG Status

Where a SAR involves a customer who is also subject to RG action (self-exclusion, operator-imposed exclusion, time-out, or operator-imposed limit), this must be noted in the internal SAR record. The customer's RG status does not change the SAR obligation but provides relevant context for the MLRO's assessment.

11.6 Quarterly Reporting Coordination

The AML Officer and the Responsible Gaming Manager coordinate input to TGC quarterly reporting under General Code of Practice Section 30.3.3, ensuring consistent customer data and avoiding duplicative or conflicting submissions to the Commission.

12. Record Keeping

The Company retains the following records for a minimum of five (5) years from the date of the relevant transaction or the end of the customer relationship, whichever is later:

- All CDD documentation and SumSub verification records;
- Age verification records and any failed-verification cases;
- Transaction records including deposit and withdrawal history and payment method details;
- EDD assessments, decisions, and supporting documentation;
- PEP risk assessments and Board approval records;
- All internal and external SARs;
- Payment method register per customer;
- Blockchain analytics screening results;
- Self-exclusion list screening matches and outcomes; and
- All Board and management AML/CFT reporting.

13. Training

All staff with AML/CFT, Payments, Fraud, or customer-facing responsibilities must complete mandatory training on commencement of employment and annually thereafter. Training is delivered via the Company's HiBob HRIS platform and completion is logged in the Training Register.

Training must cover, at minimum: the regulatory framework applicable to the Company; this Policy in full; how to identify and report suspicious activity; online gaming-specific red flags; pre-paid card and crypto risk; the touchpoints between AML and RG (Section 11); and the consequences of non-compliance.

14. Business Risk Assessment

The Company maintains a documented Business Risk Assessment ("BRA") as a standalone document, prepared in accordance with AML Regulations Section 9 and AML Code of Practice Section 10. The BRA:

- Identifies and assesses the ML/TF/PF risks specific to the Company's business model, customer base, products and services, geographies, and delivery channels;
- Documents the inherent and residual risk levels and the controls applied to mitigate them;
- Includes a documented Customer Risk Assessment methodology and a Country / Geographic Risk schedule;
- Is reviewed and updated at least annually, and whenever a material change occurs in the Company's operations, brand portfolio, payment methods, customer base, or regulatory framework;
- Is approved by the Board prior to taking effect.

The thresholds, controls, and procedures set out in this Policy are calibrated to the risks identified in the BRA. Any material change to the BRA may require corresponding amendments to this Policy. The BRA is owned by the AML Officer and is referenced in the Compliance Documentation Register.

15. Policy Governance and Review

This Policy is owned by the AML Officer and reviewed at least annually or whenever a material change occurs to the Company's business model, licence conditions, payment methods, brands, or regulatory framework. Amendments must be approved by the Board before taking effect.

Annex A - Payment Agent Subsidiaries in Scope

The following entities are subsidiaries of Neptune Projects SRL and operate as payment agents. All are in scope of this Policy.

Entity Name	Jurisdiction	Status
Sultucia Limited	Cyprus	Active
Pireneo Limited	Cyprus	Active
Inamura Limited	Cyprus	Active
Felenga Limited	Cyprus	Active
Balite Limited	Cyprus	Active
Dibona Ventures Ltd	Cyprus	Active

Annex B - Internal SAR Form

Submit completed form to the AML Officer via secure email or the designated SAR channel. Do not discuss the content with anyone else.

Field	Entry
Date of report	

Reporting staff member - name and role	
--	--

Field	Entry
Customer ID / username	
Brand(s) involved	casiny.com · vegastars.com · voltrush.com · royalerush.com
Date(s) of suspicious activity or transaction	
Nature of suspicion - describe the activity	
Amount(s) involved	
Payment method(s) involved	
Customer's RG status (if any) - e.g. self-excluded, operator-imposed limit	
Any prior flags or SARs on this customer?	Yes / No - if yes, provide details
Has any account action been taken?	Yes / No - if yes, describe
Any other relevant information	

The AML Officer will acknowledge receipt within 1 business day and provide a determination within 5 business days. Do not discuss this report with anyone else.

Annex C - EDD Checklist

This checklist must be completed by the AML Officer for every EDD case. Retain in the customer file.

#	EDD Measure	Completed / Notes
1	Customer ID confirmed - full name, DOB, address verified	
2	Source of funds documentation obtained and reviewed	
3	Source of wealth statement obtained (if cumulative deposits ≥ €5,000)	
4	Adverse media search conducted - Google + third-party tool	
5	PEP check completed and result documented	
6	Sanctions screening confirmed - no match or match reviewed	
7	All previous transactions reviewed for consistency	
8	Payment methods reviewed - all within customer's name	
9	Blockchain analytics screening completed (if any crypto transactions)	
10	RG status reviewed - coordination with RG Manager if applicable	
11	Risk assessment written and signed by AML Officer	
12	Board approval obtained (if PEP relationship)	
13	Decision: Continue / Close / SAR - documented with rationale	

Policy Sign-Off

Role	Name & Signature	Date
AML Officer / MLRO	Arvids Vitolins	
Director	Maria Luna Gonzalez Madrigal	
Board Representative		