A decorative graphic at the top of the page consisting of several overlapping, semi-transparent blue waves of varying shades, creating a sense of movement and depth.

ANTI-MONEY LAUNDERING & COUNTER FUNDING OF TERRORISM AND PROLIFERATION CDD PROCEDURE

Bluewave Interactive N.V

Document	Version	Description of Changes	Prepared By:	Reviewed By:	Review Date	Approved By	Approval Date	Next Review Date
AML/CFT/CPF CDD Procedure	1.0	Initial procedure and implementation	Compliance Officer	Chief Legal and Compliance Officer	20 th July 2026	Board of Directors	21 st July 2026	July 2027

CONTENTS

1	Introduction	4
1.1	Purpose	4
1.2	Scope	5
2.	Definition of Terms	5
3.	Regulatory Framework	6
4.	Governance and Responsibilities	7
4.1	Board of Directors	7
4.2	Senior Management	7
4.3	Compliance Function	7
4.4	MLRO	7
4.5	Operational Teams	8
I.	Customer Registration	8
II.	Customer Due Diligence	10
	CDD Threshold	10
	Identity Verification	11
	Address Verification	13
	Screening	14
	Sanctions Screening	15
	PEP Screening	15
	Adverse Media Screening	16
III.	Enhanced Due Diligence	16
IV.	PEP Enhanced Due Diligence	19
IV.	Transaction Monitoring	20
	Transaction Trigger Events	22
	Activity Trigger Events	22
	Player-to-Player (P2P) Monitoring	23
	Escalation of Alerts	25
V.	Suspicious Activity/Transaction Reporting (SAR/STR)	26
	Internal Reporting	27
	External Reporting	29
	No Tipping Off	29
VI.	Account Restriction and Account Closure	30
	Incomplete CDD	30
	Sanctions Match	30
	Termination Decision	32
	Return of Customer Funds	33
VII.	Training	35
	Induction Training	36
	Annual Refresher	36
VIII.	Record Keeping	36

Screening Result	37
Monitoring Records.....	37
STR/SAR Records	38
Retention Period.....	38
IX. Review and Update	39
Annex A- Customer Registration.....	40
Annex B- Acceptable Verification Documents	44
Annex C- Sanctions Procedure.....	45

1.1 PURPOSE

This Customer Due Diligence (“CDD”) and Know Your Customer (“KYC”) Procedure establish the processes and controls implemented by Bluewave Interactive N.V (the “Company”) for the identification, verification, risk assessment, monitoring , and ongoing management of customers in accordance with applicable Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (“AML/CFT”) requirements.

These Procedures are intended to ensure that the Company maintains effective and proportionate customer due diligence measures in accordance with applicable Anti-Money Laundering, Counter-Terrorist Financing, and Counter-Proliferation Financing (“AML/CFT”) legal and regulatory obligations, including the applicable laws, regulations, licensing conditions, and regulatory guidance governing online gaming operators in Curaçao.

The Procedures are designed to support the Company's risk-based approach to AML/CFT compliance by ensuring that customers are appropriately identified and verified, customer risks are assessed and managed, and ongoing monitoring is conducted to detect unusual or suspicious activity.

These Procedures apply to all customer relationships established by the Company and cover the full customer lifecycle, including customer onboarding, identification and verification, customer risk assessment, sanctions and PEP screening, source of funds and source of wealth reviews, ongoing monitoring, enhanced due diligence measures, trigger event reviews, and customer offboarding.

This Procedures Manual forms part of the Company's broader governance, risk management, and compliance framework and shall be applied in conjunction with the Company's:

- AML/CFT Policy;
- Business Risk Assessment (“BRA”);
- Customer Risk Assessment (“CRA”) Methodology;
- Transaction Monitoring Procedures;
- Reporting and Escalation Procedures;
- Sanctions Compliance Procedures; and
- Other related internal AML/CFT policies and procedures.

1.2 SCOPE

These Customer Due Diligence ("CDD") and Know Your Customer ("KYC") Procedures apply to all directors, officers, employees, consultants, contractors, outsourced service providers, and any other persons performing activities on behalf of the Company that involve customer onboarding, verification, risk assessment, transaction monitoring, customer reviews, or other AML/CFT-related functions.

These Procedures apply to all customers, products, services, gaming activities, payment transactions, and business relationships established or maintained by the Company and shall be complied with throughout the entire customer lifecycle.

The Procedures govern the application of customer due diligence measures from the point of customer registration and onboarding through to ongoing monitoring, periodic review, enhanced due diligence, account restriction or suspension, and termination of the customer relationship.

The Procedures apply to all customer interactions conducted through the Company's online gaming platform, including any Player-to-Player ("P2P") products, payment channels, and other services offered by the Company.

All persons within the scope of these Procedures are responsible for ensuring that customer due diligence measures are applied in accordance with the Company's AML/CFT framework and applicable legal and regulatory requirements.

2. DEFINITION OF TERMS

"AML/CFT" means anti-money laundering and counter-funding of terrorism

"Board" or "Board of Directors" means the Board of Directors of the Company.

"BRA" means the Company's Business Risk Assessment relating to money laundering, terrorist financing, proliferation financing, sanctions, and related AML/CFT risks.

"CDD" means Customer Due Diligence measures carried out in accordance with applicable AML/CFT obligations.

"Company" means Bluewave Interactive N.V

"CRA" means Customer Risk Assessment.

"EDD" means Enhanced Due Diligence.

"FATF" means the Financial Action Task Force.

"FIU" means the Curacao Financial Intelligence Unit

"ML" means money laundering.

“ML/FT/PF” means money laundering, terrorist financing, and proliferation financing collectively.

“MLRO” means the Money Laundering Reporting Officer appointed by the Company in accordance with applicable AML/CFT requirements.

“PEP” means Politically Exposed Person and includes family members and known close associates where applicable.

“Personnel” means all individuals engaged by the Company, including directors, officers, employees, secondees, consultants, contractors, temporary staff, the MLRO, members of the Compliance Function, and any other persons acting on behalf of the Company.

“PF” means proliferation financing.

“RBA” means risk-based approach.

“Sanctions” means restrictive measures, sanctions regimes, or financial sanctions imposed by the United Nations, European Union, Curacao, or any other applicable competent authority.

“Senior Management” means the persons responsible for the day-to-day management and operation of the Company.

“STR” or “SAR” means a Suspicious Transaction Report or Suspicious Activity Report submitted internally or externally in accordance with applicable AML/CFT obligations.

“TF” means terrorist financing.

3. REGULATORY FRAMEWORK

This AML/CFT Policy is established in accordance with the applicable legal, regulatory, and supervisory framework governing the prevention of money laundering, terrorist financing, proliferation financing, sanctions compliance, as amended from time to time

In particular, this Policy has been developed having regard to inter alia:

- National Ordinance on Identification when rendering Services (“NOIS”)
- National Ordinance on the Reporting Unusual Transactions (“NORUT”)
- Sanctions National Ordinance
- Kingdom Sanction Act
- Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction

4. GOVERNANCE AND RESPONSIBILITIES

4.1 BOARD OF DIRECTORS

The Board of Directors are responsible for:

- Approving the Business Risk Assessment
- Defining and overseeing the Company's risk appetite ensuring adequate resources for AML/CFT compliance

The Board shall ensure that the MLRO and Compliance Function are provided with sufficient authority, independence, resources, and access to training effectively discharge their responsibilities

4.2 SENIOR MANAGEMENT

The Senior Management is responsible for:

- Implementing controls at an operational level
- Ensuring day-to-day effectiveness of AML/CFT measures

4.3 COMPLIANCE FUNCTION

The Compliance Function is responsible for:

- Monitoring adherence for this policy and the overall AML/CFT framework
- Performing periodic testing and reviews, including independent testing of the effectiveness of Controls and reporting deficiencies to Senior Management and the Board
- Tracking regulatory and legislative developments

4.4 MLRO

The Money Laundering Reporting Officer is responsible for:

- Receiving, analysing and assessing internal suspicious reports and determining whether to submit STRs/SARs to the FIU Curacao
- Ensuring effective internal reporting procedures and acting as the central point of contact with the FIU
- Contributing to the development and periodic review of the BRA in coordination with the Compliance Function and Senior Management and the Board
- Tracking Regulatory and legislative developments

4.5 OPERATIONAL TEAMS

Employees involved in customer onboarding, customer support, payments, fraud prevention, responsible gaming, or other operational functions shall support the implementation of these Procedures.

- Operational teams shall:
- Obtain required customer information and documentation;
- Identify and escalate unusual or suspicious activity;
- Support customer due diligence and verification processes;
- Comply with account restriction and escalation requirements; and
- Cooperate with Compliance and the MLRO in the performance of AML/CFT reviews.

I. CUSTOMER REGISTRATION

Customer registration is the process by which a prospective customer creates a gaming account through the Company's online gaming platform. The objective of the registration process is to establish the customer's profile, capture the minimum information required to initiate a business relationship, and enable the application of subsequent AML/CFT controls, including customer screening, customer due diligence, and customer risk assessment.

The registration process is completed electronically through the Company's gaming platform and is supported by automated validation controls to ensure that mandatory information is provided before an account is created.

Registration Process

The registration process shall be completed in the following sequence:

Step 1 – Account Registration

The prospective customer accesses the Company's registration page and completes the online registration form.

The registration system shall require all mandatory fields to be completed before the application can be submitted. The customer shall not be permitted to proceed where mandatory information is incomplete.

Step 2 – Collection of Registration Information

The registration system shall capture the information provided by the customer and create an electronic customer profile.

The information collected during registration shall be recorded within the customer management system and retained as part of the customer's permanent record.

Step 3 – Customer Declarations

Prior to submitting the registration, the customer shall electronically confirm the website's Terms and Conditions which includes the following:

- all information provided is true, accurate and complete;
- the account is being opened and operated solely on their own behalf;
- they have reached the minimum legal age to participate in gambling activities;
- they agree to the Company's Terms and Conditions; and
- they acknowledge the Company's Privacy Policy.

The registration system shall record the date, time and version of the declarations accepted by the customer.

Step 4 – System Validation

Upon submission of the registration form, the registration system shall automatically perform validation checks, including, where applicable:

- confirmation that all mandatory registration fields have been completed;
- validation of email address format;
- validation of mobile telephone number format;
- duplicate account detection;
- minimum age validation;
- country and jurisdiction verification;
- IP address capture;
- device identification and fingerprinting (where implemented); and
- fraud prevention controls configured within the platform.

Any validation failures shall generate an exception and prevent the registration from progressing until the exception has been resolved.

Step 5 – Customer Account Creation

Where the registration has successfully passed all automated validation checks, the system shall:

- create the customer account;
- assign a unique Customer Identification Number (Customer ID);
- create the customer's electronic profile; and
- transfer the account to the initial screening and Customer Due Diligence process.

Creation of the customer account does not constitute completion of Customer Due Diligence and does not automatically permit unrestricted use of the gaming platform.

Registration Exceptions

Where the registration process identifies an exception, the account shall be referred for manual review by the appropriate operational team prior to the customer depositing funds and playing on the platform.

Examples of registration exceptions include:

- incomplete or inconsistent customer information;
- suspected duplicate accounts;
- underage registration attempts;
- registration from prohibited or restricted jurisdictions;
- failed automated validation checks;
- suspected fraudulent registration attempts; or
- any other system-generated alert requiring further review.

The outcome of the manual review shall be documented within the customer management system together with any actions taken before the customer is permitted to play

II. CUSTOMER DUE DILIGENCE

CDD THRESHOLD

The Company applies a risk-based approach to Customer Due Diligence ("CDD"). While customers may register and establish an account with the minimum registration information, full CDD shall be initiated once a customer reaches the applicable CDD threshold or where earlier intervention is required based on the customer's risk profile or other trigger events.

For the purposes of these Procedures, the CDD threshold is reached when a customer's cumulative deposits equal or exceed **NAf. 4,000**, or the equivalent value in another currency, calculated from the commencement of the business relationship.

The threshold shall be calculated automatically by the Company's gaming platform and shall aggregate all qualifying deposits made by the customer. The monitoring system shall continuously track customer deposits and generate an automated alert immediately upon the threshold being reached or exceeded.

Upon receipt of a CDD threshold alert, the following operational procedures shall apply:

Step 1 – Automated Threshold Detection

The system shall automatically identify customers whose cumulative deposits have reached or exceeded the applicable threshold and generate a CDD review task within the Compliance case management system.

Step 2 – Account Restriction

Pending completion of the required CDD measures, the customer's account shall automatically be subject to the following restrictions:

- No further deposits shall be permitted.
- Withdrawals shall be restricted in accordance with the Company's AML/CFT Policy and applicable regulatory requirements.
- The customer may continue to participate in gaming activities using the existing account balance, where permitted by law and internal policy.

Where the threshold is reached as a result of a withdrawal request, the account shall be restricted from further gambling activity until the required CDD measures have been completed.

Step 3 – Customer Notification

The customer shall be notified through the Company's approved communication channels that identity verification and additional customer due diligence are required before normal account functionality can resume.

The notification shall specify the documentation or information required and, where applicable, provide instructions for secure document submission.

Step 4 – Risk Team Review

The Compliance Team shall initiate the CDD process by:

- reviewing the customer's information;
- initiating identity verification;
- verifying the customer's residential address;
- completing or updating the Customer Risk Assessment ("CRA");
- performing sanctions, PEP, and adverse media screening;
- determining whether Source of Funds ("SOF"), Source of Wealth ("SOW"), or Enhanced Due Diligence ("EDD") measures are required; and
- recording all actions, findings, and decisions within the customer management system.

IDENTITY VERIFICATION

Identity Verification is performed to confirm that the customer is the individual they claim to be and to provide the Company with reasonable assurance that it is establishing and maintaining a business relationship with the correct person.

Identity verification shall be completed by the Compliance Team following the triggering of Customer Due Diligence requirements or earlier where required under the Company's risk-based approach.

Identity Verification Process

The Compliance Team shall verify the customer's identity using reliable and independent documentation, electronic verification solutions, or other approved verification methods.

Identity verification shall, at a minimum, confirm the following customer information:

- Full legal name;
- Date of birth;
- Nationality;
- Place of birth (where collected);
- Identification document number;
- Expiry date of the identification document; and
- Photograph of the customer.

The customer shall be requested to upload a valid government-issued photographic identification document through the Company's approved verification platform.

Accepted identity documents include:

- Passport;
- National Identity Card; or
- Driver's Licence

The document submitted must:

- be valid and unexpired;
- display the customer's full name;
- contain a clear photograph of the customer;
- include the customer's date of birth;
- contain a unique document number;
- be issued by a recognised government authority;
- be fully visible, legible and of sufficient quality for review; and
- not show signs of alteration, manipulation, or damage.

Verification Review

The Risk Team shall review the submitted documentation to verify that:

- the identity document belongs to the customer;
- the information matches the customer's registration details;
- the document is authentic and appears genuine;
- the document has not expired;
- the photograph reasonably matches the individual completing the verification process;
- there are no inconsistencies or indications of document tampering; and
- there are no discrepancies requiring further investigation.

Where electronic identity verification or biometric verification is available, the verification results shall be reviewed as part of the overall identity verification process.

Verification Exceptions

Where identity verification cannot be completed successfully, the Risk Team shall determine whether additional information or documentation is required.

Examples include:

- poor quality or illegible documents;
- expired identification documents;
- inconsistencies between the registration information and the identification document;
- suspected forged or altered documentation;
- unsuccessful biometric or liveness verification;
- inability to verify the customer's identity through approved verification methods; or
- any other circumstance giving rise to concerns regarding the customer's identity.

Where necessary, the customer may be requested to provide:

- an alternative government-issued identification document;
- a higher-quality copy of the identification document;
- a live selfie or biometric verification;
- a photograph of the customer holding the identification document; or
- any additional documentation considered necessary to verify the customer's identity.

ADDRESS VERIFICATION

Address Verification is performed to confirm the customer's current residential address and to support the Company's Customer Due Diligence ("CDD") obligations. Address verification assists the Company in validating the customer's country of residence, assessing geographical risk, and ensuring that customer records remain accurate and up to date.

Address verification shall be completed where required under the Company's AML/CFT Policy, Customer Risk Assessment, or where the customer reaches the applicable CDD threshold or is otherwise subject to enhanced due diligence measures.

Address Verification Process

The Risk Team shall request the customer to provide documentary evidence of their current residential address through the Company's approved verification platform.

The document submitted must clearly display:

- The customer's full name;
- The residential address;
- The name of the issuing organisation or authority; and
- The invoice date of issue

Unless otherwise approved by the Risk Team, proof of address documents shall have been issued within the previous six (6) months or three months (3) for High-risk customers

Acceptable proof of address documents include, but are not limited to:

- Utility bill (electricity, water, gas, fixed-line telephone or internet);
- Bank or credit card statement;
- Government-issued correspondence;
- Local authority or tax authority correspondence;
- Official residence certificate or registration document;
- Tenancy agreement or lease agreement, where supported by independent verification

Electronic statements or documents downloaded from official customer portals may be accepted where their authenticity can be reasonably established.

Verification Review

The Risk Team shall review the submitted document to confirm that:

- the customer's name matches the registered account details;
- the residential address matches the information recorded within the customer profile, or any differences have been satisfactorily explained;
- the document has been issued by a recognised organisation or competent authority;
- the document falls within the Company's accepted validity period;
- the document is complete, legible, and free from signs of alteration or manipulation; and
- the address is located within a jurisdiction that is not prohibited or otherwise subject to restrictions under the Company's AML/CFT framework.

Verification Exceptions

Where the submitted documentation is insufficient to verify the customer's residential address, the Risk Team shall request additional documentation or clarification.

Examples of verification exceptions include:

- the address document is older than the accepted validity period;
- the customer's name does not match the registered account information;
- the residential address differs from the address recorded during registration;
- the document is incomplete, illegible, or appears to have been altered;
- the issuing organisation cannot be reasonably verified; or
- there are inconsistencies that require further investigation.

Where necessary, the customer may be requested to provide an alternative proof of address document or additional information to support the

SCREENING

Customer screening is conducted to identify whether a customer presents an elevated Money Laundering, Terrorist Financing, Proliferation Financing ("ML/TF/PF"), sanctions, bribery, corruption, or reputational risk prior to, and throughout, the business relationship.

The Company utilises a risk-based approach to customer screening and shall perform sanctions, Politically Exposed Person ("PEP"), and adverse media screening using the Company's approved screening solution.

Customer screening shall be performed:

- upon customer registration or prior to establishing the business relationship;
- upon completion of Customer Due Diligence ("CDD");
- prior to establishing or continuing a relationship with a High-Risk Customer;
- whenever there is a material change to the customer's profile;
- upon the occurrence of a trigger event requiring reassessment;
- periodically in accordance with the Company's ongoing monitoring programme; and
- whenever new sanctions lists, PEP data, or adverse media information become available through the Company's screening provider.

The Compliance Team is responsible for reviewing all screening results, investigating potential matches, documenting the outcome of the review, and determining whether additional due diligence or escalation is required.

Screening Outcomes

Following completion of customer screening, the Compliance Team shall record one of the following outcomes:

- **Cleared** – No matches or concerns identified.
- **False Positive** – Potential match investigated and determined not to relate to the customer.

SANCTIONS SCREENING

Sanctions Screening

The Company shall screen all customers against applicable international sanctions lists before establishing or continuing a business relationship.

At a minimum, sanctions screening shall include:

- United Nations Security Council ("UN") Sanctions Lists;
- European Union ("EU") Consolidated Sanctions List;
- Any Curaçao sanctions or designated persons list, where applicable; and
- Any additional sanctions lists made available through the Company's approved screening provider.

Where a potential sanctions match is identified:

- the customer account shall immediately be referred to the Compliance Team;
- no further transactions shall be permitted until the alert has been reviewed;
- Compliance shall determine whether the match is a false positive or a potential true match;
- where necessary, additional information or documentation shall be obtained from the customer;
- confirmed or suspected sanctions matches shall be escalated immediately to the MLRO for further assessment and any required regulatory action.

PEP SCREENING

All customers shall be screened to determine whether they are a Politically Exposed Person ("PEP"), a family member of a PEP, or a close associate of a PEP.

Where a customer is identified as a PEP, family member, or close associate, the Risk Team shall:

- verify the customer's PEP status;
- determine the nature of the public function held;
- assess the ML/TF/PF risk associated with the customer;
- determine whether Enhanced Due Diligence ("EDD") is required;
- obtain Source of Funds ("SOF") and Source of Wealth ("SOW") information where appropriate;
- escalate the relationship for approval in accordance with the Company's AML/CFT procedures; and

- ensure the customer is subject to enhanced ongoing monitoring.

PEP status shall not automatically prevent the establishment or continuation of a business relationship; however, the relationship shall only proceed where the associated risks can be appropriately managed.

ADVERSE MEDIA SCREENING

The Company shall perform adverse media screening to identify credible information linking a customer to financial crime, fraud, money laundering, terrorist financing, corruption, organised crime, sanctions violations, or other criminal activity.

The Compliance Team shall review adverse media results to determine:

- the credibility and reliability of the source;
- the relevance of the information to the customer;
- whether the information indicates an elevated ML/TF/PF risk;
- whether Enhanced Due Diligence is required; and
- whether the relationship should be escalated, restricted, or declined.

Unverified allegations or media reports from unreliable sources shall not, on their own, result in an adverse customer decision. All screening results shall be assessed using professional judgement and documented accordingly.

III. ENHANCED DUE DILIGENCE

Enhanced Due Diligence ("EDD") is a risk-based process applied to customers presenting a higher risk of Money Laundering, Terrorist Financing or Proliferation Financing ("ML/TF/PF"). The objective of EDD is to obtain a greater understanding of the customer, the origin of the customer's funds and wealth, and the nature of the customer's gambling activity in order to determine whether the business relationship can continue within the Company's risk appetite.

EDD shall be performed by the Compliance Team and, where required, escalated to the MLRO for review and approval.

EDD Trigger Events

EDD shall be initiated where one or more of the following circumstances apply:

- the customer is classified as High Risk following the Customer Risk Assessment;
- the customer is identified as a Politically Exposed Person ("PEP"), family member or close associate;
- the customer resides in or transacts from a high-risk or sanctioned jurisdiction;
- unusual or suspicious transactions or gambling activity have been identified;
- transaction activity is inconsistent with the customer's known profile;
- the customer exceeds the Company's internal financial thresholds;
- there are concerns regarding the legitimacy of the customer's Source of Funds ("SOF") or Source of Wealth ("SOW");
- adverse media or other negative intelligence identifies elevated ML/TF/PF risk;
- there are concerns regarding third-party funding or beneficial ownership of funds; or

- the MLRO or Compliance Team determines that additional due diligence is required.

Enhanced Due Diligence Procedure

Upon identification of an EDD trigger, the Risk Team shall:

Step 1 – Review the Customer Profile

The Compliance Analyst shall review:

- Customer Risk Assessment;
- customer registration information;
- previous CDD records;
- transaction history;
- gambling behaviour;
- payment methods;
- previous compliance reviews; and
- any existing monitoring alerts.

The purpose of the review is to determine the nature of the identified risk and establish the scope of the enhanced due diligence required.

Step 2 – Enhanced Screening

The customer shall be subject to enhanced sanctions, PEP, adverse media, and other intelligence screening using the Company's approved screening solution.

Where new adverse information is identified, the Risk Team shall determine whether further investigation or escalation is required.

Step 3 – Source of Funds Assessment

Where appropriate, the Risk Team shall request evidence demonstrating the origin of the funds used for the customer's gambling activity.

The assessment shall determine whether the customer's deposits and gambling activity are consistent with the declared source of funds and known financial profile.

Examples of acceptable documentation include:

- recent payslips;
- employment confirmation;
- bank statements;
- business income documentation;
- investment statements;
- property sale agreements;
- inheritance documentation;
- cryptocurrency transaction records (where applicable); or

- other reliable documentation supporting the origin of the deposited funds.

Step 4 – Source of Wealth Assessment

Where the customer's overall financial position cannot reasonably explain the level of gambling activity, or where the customer is identified as presenting a higher ML/TF/PF risk, the Compliance Team shall obtain information demonstrating how the customer's overall wealth has been accumulated.

The assessment shall consider the customer's occupation, business interests, declared income, assets, publicly available information, and any supporting documentation provided.

Source of Wealth documentation may include:

- tax returns;
- audited financial statements;
- business ownership records;
- investment portfolios;
- property ownership or sale documentation;
- inheritance records; or
- other documentation considered sufficient to establish the customer's accumulated wealth.

Step 5 – Assessment and Decision

The Risk Team shall assess whether:

- the information provided is complete and internally consistent;
- the customer's financial profile supports the level of gambling activity;
- the Source of Funds and Source of Wealth are reasonable and credible;
- any residual ML/TF/PF risks remain acceptable; and
- additional information or clarification is required.

Where the information provided is insufficient or raises further concerns, additional documentation may be requested before a final decision is reached.

Escalation

EDD cases shall be escalated to the MLRO where:

- Source of Funds or Source of Wealth cannot be satisfactorily established;
- significant inconsistencies remain unresolved;
- suspicious activity has been identified;
- sanctions or PEP concerns require further assessment;
- the customer falls outside the Company's defined risk appetite; or
- consideration is being given to terminating the business relationship or submitting an internal or external suspicious activity report.

IV. PEP ENHANCED DUE DILIGENCE

Customers identified as Politically Exposed Persons ("PEPs"), their family members, or close associates shall be subject to Enhanced Due Diligence ("EDD") measures in accordance with the Company's AML/CFT Policy.

Where a customer is confirmed as a PEP, the standard Enhanced Due Diligence procedures set out in Section 4.X of this Manual shall be completed together with the additional requirements specified below.

PEP Enhanced Due Diligence Procedure

Upon confirmation of a customer's PEP status, the Compliance Team shall:

Step 1 – Confirm PEP Status

The Compliance Team shall review the screening results to confirm whether the customer is:

- a domestic PEP;
- a foreign PEP;
- an individual entrusted with a prominent public function by an international organisation;
- a family member of a PEP; or
- a close associate of a PEP.

False positive matches shall be documented and closed in accordance with the Company's Screening Procedures.

Step 2 – Complete Enhanced Due Diligence

The Compliance Team shall complete the Enhanced Due Diligence procedures described in Section 4.X, including:

- enhanced customer profile review;
 - enhanced sanctions and adverse media screening;
 - Source of Funds assessment;
 - Source of Wealth assessment;
 - customer risk reassessment; and
 - documentation of all findings.
-

Step 3 – Senior Management Approval

Before establishing or continuing the business relationship, the Compliance Team shall prepare a PEP assessment summary and submit the case to Senior Management for approval.

The submission shall include:

- the customer's risk profile;
-

- details of the public function held;
- Source of Funds assessment;
- Source of Wealth assessment;
- screening results;
- adverse media findings;
- transaction profile;
- Compliance recommendation; and
- any additional risk factors identified during the review.

Senior Management shall determine whether the ML/TF/PF risks associated with the customer can be appropriately managed and whether the business relationship may be established or continued.

The approval or rejection decision shall be documented within the customer management system.

Step 4 – Enhanced Ongoing Monitoring

Where a PEP relationship is approved, the customer shall remain subject to enhanced ongoing monitoring throughout the duration of the business relationship.

Enhanced monitoring shall include:

- more frequent customer risk reviews;
- periodic review of Source of Funds and Source of Wealth;
- enhanced transaction monitoring;
- periodic sanctions, PEP, and adverse media re-screening;
- review of changes to the customer's public function or political exposure; and
- review of any unusual or suspicious transaction or gambling activity.

The frequency of ongoing reviews shall be determined based on the customer's overall ML/TF/PF risk rating and documented within the Customer Risk Assessment.

IV. TRANSACTION MONITORING

The Company maintains automated and manual transaction monitoring controls to identify customer transactions that may present an elevated Money Laundering, Terrorist Financing, or Proliferation Financing ("ML/TF/PF") risk.

Transaction trigger events are designed to identify activity that deviates from the customer's expected profile, exceeds predefined risk thresholds, or otherwise warrants additional review by the Compliance Team.

Where a transaction trigger event is identified, the monitoring system shall generate an alert for review by the Risk Team.

Step 1 – Review the Alert

The AML Analyst shall review the alert to determine:

- the transaction(s) that triggered the alert;
 - the customer's current risk rating;
 - recent gambling activity;
 - deposit and withdrawal history;
 - payment methods used;
 - previous monitoring alerts;
 - previous Customer Due Diligence ("CDD") reviews; and
 - any previous Source of Funds ("SOF") or Enhanced Due Diligence ("EDD") assessments.
-

Step 2 – Assess the Activity

The Risk Team shall determine whether the transaction activity is:

- consistent with the customer's known profile;
- supported by previous gambling behaviour;
- consistent with the customer's declared Source of Funds or Source of Wealth;
- indicative of normal recreational gambling; or
- indicative of unusual or potentially suspicious activity.

Where necessary, additional customer information or documentation may be requested.

Step 3 – Determine Required Action

Following the review, the ML Analyst shall determine whether to:

- close the alert with no further action;
- update the customer's risk profile;
- perform a Customer Due Diligence review;
- initiate Enhanced Due Diligence;
- request Source of Funds documentation;
- request Source of Wealth documentation;
- apply account restrictions;
- escalate the matter to the MLRO; or
- commence an internal unusual activity investigation.

All actions and decisions shall be documented within the customer management system.

TRANSACTION TRIGGER EVENTS

Without limitation, the following transaction activities shall trigger a Compliance review:

- Cumulative customer deposits reaching the Company's CDD threshold.
- Single or cumulative transactions exceeding internal monitoring thresholds.
- Significant increases in deposit or withdrawal activity inconsistent with the customer's historical profile.
- Rapid deposits followed by immediate withdrawals with minimal or no genuine gambling activity.
- Large withdrawals shortly after substantial deposits.
- Multiple deposits followed by limited wagering activity.
- Frequent deposits and withdrawals over a short period.
- Structuring transactions to avoid internal monitoring thresholds.
- Use of multiple payment methods without a reasonable explanation.
- Frequent changes to registered payment methods.
- Use of payment methods registered to third parties.
- Repeated failed deposit or withdrawal attempts.
- Multiple cancelled withdrawal requests followed by additional gambling activity.
- Unusual transaction velocity or frequency.
- High-value transactions inconsistent with the customer's known financial profile.
- Transactions involving high-risk jurisdictions.
- Transactions involving virtual assets or other higher-risk payment methods, where permitted.
- Customer activity indicating potential chip dumping, value transfer, or collusion within Player-to-Player ("P2P") products.
- Any transaction identified by the monitoring system as unusual based on predefined risk scenarios or behavioural models.

The above trigger events are not exhaustive. The Compliance Team may initiate a review whenever any transaction or pattern of activity appears unusual, inconsistent with the customer's profile, or otherwise presents an elevated ML/TF/PF risk.

ACTIVITY TRIGGER EVENTS

Without limitation, the following customer activities shall trigger a Compliance review:

Customer Profile

- Material changes to the customer's personal information or residential address.
- Change of nationality or country of residence.
- Changes to occupation or employment status, where known.
- Expiry or replacement of identity verification documents.
- Changes to the customer's PEP status, sanctions status, or adverse media profile.

Account Activity

- Extended periods of account inactivity followed by significant gambling activity.
- Significant changes in gambling frequency, wagering behaviour, or gaming preferences.
- Multiple customer accounts linked through common identifiers.
- Indicators of account sharing or account takeover.
- Frequent changes to account credentials or profile information.

Customer Conduct

- Failure or refusal to provide requested CDD or EDD documentation.
- Submission of inconsistent, incomplete, or misleading information.
- Attempts to circumvent the Company's verification or AML/CFT controls.
- Uncooperative or evasive responses to Compliance enquiries.

Gaming Activity

- Gambling behaviour inconsistent with the customer's historical activity.
- Gaming activity lacking an apparent recreational purpose.
- Patterns indicative of collusion or coordinated gameplay.
- Activity suggesting value transfer through gaming products.
- Unusual Player-to-Player ("P2P") activity, including repeated interactions with the same players or activity indicative of chip dumping or collusion.

Technical Indicators

- Frequent changes to devices, IP addresses, or geolocation inconsistent with the customer's profile.
- Simultaneous access from multiple locations.
- Use of anonymising technologies where prohibited or inconsistent with the customer's known profile.

The above trigger events are not exhaustive. The Compliance Team may initiate a review whenever customer activity appears inconsistent with the Company's knowledge of the customer or otherwise presents an elevated ML/TF/PF risk.

PLAYER-TO-PLAYER (P2P) MONITORING

The Risk Team shall review P2P activity where monitoring systems generate alerts or where unusual gameplay patterns are identified through manual review.

Step 1 – Review Customer Activity

The AML Analyst shall review:

- the customer's gaming history;
- counterparties involved in the gameplay;
- deposits and withdrawals associated with the activity;
- game type and stake levels;
- timing and frequency of gameplay;

- customer risk rating;
- previous compliance reviews; and
- previous monitoring alerts.

The purpose of the review is to determine whether the gameplay is consistent with legitimate recreational gaming.

Step 2 – Assess the Activity

The Risk Team shall assess whether the gameplay:

- is consistent with the customer's historical gaming behaviour;
- demonstrates a legitimate commercial purpose;
- indicates possible value transfer between players;
- suggests collusion or coordinated gameplay;
- appears designed to facilitate the movement of funds rather than genuine gaming;
- is supported by the customer's known financial profile; and
- presents indicators of ML/TF/PF or fraud.

Where appropriate, additional information or documentation may be requested from the customer.

Step 3 – Determine Appropriate Action

Following completion of the review, the Risk Team shall determine whether to:

- close the review with no further action;
- update the Customer Risk Assessment;
- initiate Customer Due Diligence;
- initiate Enhanced Due Diligence;
- request Source of Funds or Source of Wealth information;
- apply restrictions to the customer's account or P2P functionality;
- escalate the matter to the MLRO; or
- commence an internal unusual activity investigation.

All actions taken shall be documented within the customer management system.

P2P Monitoring Indicators

Without limitation, the following activities shall trigger an AML review:

- Repeated gameplay involving the same player or group of players.
 - Repeated losses or wins between the same counterparties without an apparent gaming rationale.
-

- Chip dumping or deliberate transfer of value through gameplay.
- Coordinated betting or gameplay suggestive of collusion.
- Gameplay involving multiple linked or associated customer accounts.
- Minimal or no genuine competitive gameplay prior to significant withdrawals.
- Disproportionate winnings or losses inconsistent with expected game outcomes.
- Rapid movement of funds between multiple P2P participants.
- Significant changes in P2P activity inconsistent with the customer's historical behaviour.
- P2P gameplay involving customers from higher-risk jurisdictions.
- Use of multiple accounts, devices, or IP addresses to facilitate gameplay.
- Activity indicative of account sharing or third-party account operation.
- Any gameplay identified by the Company's monitoring systems as presenting an elevated ML/TF/PF or fraud risk.

The above indicators are not exhaustive. The Risk Team may review any P2P activity that appears unusual, inconsistent with the customer's profile, or otherwise presents an elevated ML/TF/PF risk.

ESCALATION OF ALERTS

The Risk Team shall escalate the matter to the MLRO where:

- the activity cannot be reasonably explained;
- unusual or suspicious activity has been identified;
- Source of Funds or Source of Wealth cannot be satisfactorily established;
- sanctions concerns have been identified;
- a confirmed PEP presents an unacceptable risk;
- there are indications of fraud, collusion, account sharing, or value transfer;
- multiple monitoring alerts indicate an increasing ML/TF/PF risk; or
- the customer falls outside the Company's defined risk appetite.

The Compliance Team shall prepare an escalation summary including:

- customer details;
- summary of the alert;
- chronology of events;
- investigation performed;
- supporting documentation;
- customer explanations (where applicable);
- Compliance assessment; and
- recommendation for further action.

Step 5 – MLRO Review

The MLRO shall independently review the information provided and determine the appropriate course of action.

The MLRO may:

- close the alert with no further action;
- request additional investigation;
- require Enhanced Due Diligence;
- request additional Source of Funds or Source of Wealth documentation;
- update the customer's risk classification;
- maintain or apply account restrictions;
- recommend termination of the business relationship;
- initiate an Internal Unusual Activity Report; or
- determine whether an external report to the FIU Curaçao is required.

The rationale supporting the MLRO's decision shall be documented within the case management system.

V. SUSPICIOUS ACTIVITY/TRANSACTION REPORTING (SAR/STR)

The Company shall implement and maintain effective procedures for the identification, internal reporting, assessment, and external reporting of suspicious activity, in accordance with applicable AML/CFT laws and regulations.

All Personnel shall remain vigilant to indicators of money laundering or terrorist financing (“ML/FT”) and shall promptly report any knowledge, suspicion, or reasonable grounds to suspect ML/FT to the Money Laundering Reporting Officer (“MLRO”) without delay

An unusual transaction is a transaction inconsistent with the player’s profile. The following transactions or intended transactions are deemed unusual and are the following but not limited to;

A. Suspicious Transactions

- Significant deposits or withdrawals inconsistent with the customer's known profile or expected activity.
- Sudden increases in deposit, wagering, or withdrawal activity.
- Rapid deposits followed by withdrawals with little or no gambling activity.
- Frequent deposits followed by minimal-risk wagering activity.
- Multiple deposits or withdrawals conducted within a short period of time.
- Transactions structured to avoid internal monitoring thresholds or regulatory reporting requirements.
- Use of multiple payment methods without a reasonable explanation.
- Frequent changes to payment methods, withdrawal destinations, or banking details.
- Deposits or withdrawals involving third-party payment methods.
- Transactions involving higher-risk jurisdictions or unusual payment flows.
- Transactions lacking an apparent economic or lawful purpose.

B. Suspicious Activity

- Gambling activity inconsistent with the customer's known profile, source of funds, or source of wealth.
- Significant changes in gambling behaviour without a reasonable explanation.
- Unusually high wagering volumes or turnover.
- Sudden transition from low-value to high-value gambling activity.
- Patterns of activity inconsistent with the customer's historical behaviour.
- Repeated attempts to circumvent account limits, verification requirements, or other controls.
- Activity inconsistent with the customer's declared occupation, income level, or financial circumstances.
- Behaviour suggesting that gambling activity is being used primarily to transfer, move, or disguise funds.

The presence of one or more indicators does not automatically mean that money laundering, terrorist financing, or other criminal activity has occurred. However, such indicators shall trigger an appropriate review and, where necessary, escalation to the MLRO for further assessment.

INTERNAL REPORTING

Step 1 – Identification of Unusual or Suspicious Activity

An internal report shall be submitted whenever an employee identifies activity that:

- appears inconsistent with the customer's known profile;
- cannot be reasonably explained following review;
- presents indicators of ML/TF/PF, fraud, collusion, or other financial crime;
- generates significant AML monitoring alerts;
- involves suspected sanctions evasion;
- involves suspected third-party account use or value transfer;
- involves falsified or fraudulent documentation; or
- otherwise gives rise to reasonable grounds for concern.

The obligation to submit an internal report applies regardless of the value of the transaction or whether the activity is completed or merely attempted.

Step 2 – Immediate Internal Escalation

The employee identifying the activity shall immediately notify the Compliance Team using the Company's approved Internal Unusual Activity Report ("IUAR") process.

Where the concern is identified by a member of the Compliance Team, the matter shall be documented and referred directly to the MLRO where appropriate.

Employees shall not investigate the matter independently beyond obtaining information necessary to explain the reason for the internal report.

Step 3 – Preparation of the Internal Report

The employee or AML Analyst shall prepare an Internal Unusual Activity Report containing, where applicable:

- Customer Identification Number;
- customer name;
- date of identification;
- description of the activity;
- reason for concern;
- relevant transaction details;
- products involved;
- payment methods;
- supporting documentation;
- monitoring alerts generated;
- actions already taken; and
- any explanation provided by the customer.

The report shall contain objective facts and observations only.

Employees shall not speculate, make accusations, or express conclusions regarding whether money laundering or terrorist financing has occurred.

Step 4 – Submission to the MLRO

The completed Internal Unusual Activity Report shall be submitted to the MLRO without undue delay.

The Risk Team shall ensure that all supporting information relevant to the report is included before submission.

Where additional information becomes available after submission, it shall be provided to the MLRO as soon as practicable.

Step 5 – Interim Account Controls

Pending the MLRO's assessment, the Risk Team may implement appropriate risk mitigation measures, including:

- enhanced transaction monitoring;
- Enhanced Due Diligence;
- temporary account restrictions;
- suspension of withdrawals where permitted by law;
- suspension of specific gaming products;
- continued monitoring of customer activity; or

- any other control considered necessary to mitigate ML/TF/PF risk.

The application of interim controls shall be proportionate to the identified risk and documented within the customer record.

Confidentiality

All Internal Unusual Activity Reports, supporting documentation, investigations, and related correspondence shall be treated as strictly confidential.

Information relating to an internal report shall only be disclosed to employees who require access for the purposes of performing their AML/CFT responsibilities.

Employees shall not disclose, either directly or indirectly, that an internal report has been submitted or that an investigation is being conducted.

Outcome

Following submission of an Internal Unusual Activity Report, responsibility for the investigation and determination of any external reporting obligation transfers to the MLRO.

The MLRO shall assess the information in accordance with the Company's **MLRO Investigation Procedure** and determine whether:

- no further action is required;
- additional investigation is necessary;
- further Customer Due Diligence or Enhanced Due Diligence is required; or
- an external report should be submitted to the FIU Curaçao.

EXTERNAL REPORTING

Where the MLRO determines that there are reasonable grounds for suspicion, a report shall be submitted promptly to the competent authority, in accordance with applicable legal and regulatory requirements.

The Company shall ensure that such reporting is carried out without undue delay and that all relevant information is included in the report

NO TIPPING OFF

Personnel shall not disclose to the customer or any third party that:

- a suspicion has been formed;
- an internal report has been made; or
- a report has been submitted to a competent authority.

Any breach of this prohibition may constitute a criminal offence and shall be subject to disciplinary action.

VI. ACCOUNT RESTRICTION AND ACCOUNT CLOSURE

The Company shall not establish or continue a business relationship where it is unable to comply with its Customer Due Diligence ("CDD") obligations or where the risks associated with the customer relationship cannot be adequately managed.

The Company may restrict, suspend, or terminate a customer relationship where:

- Required CDD information or documentation is not provided within 30 days timeframe;
- Customer identity cannot be satisfactorily verified;
- Source of Funds ("SOF") or Source of Wealth ("SOW") requirements cannot be fulfilled where required;
- The customer refuses to cooperate with CDD, EDD, or ongoing monitoring requirements;
- The customer provides false, misleading, incomplete, or inconsistent information;
- The Company is unable to adequately mitigate identified ML/TF/PF risks; or
- Continued operation of the account would expose the Company to unacceptable regulatory, legal, financial crime, or reputational risk.

INCOMPLETE CDD

The Risk Team shall identify customers who have failed to complete the required CDD measures within thirty (30) day, including where:

- the customer has reached the applicable CDD threshold;
- requested identity or address verification documents have not been provided;
- Source of Funds ("SOF") or Source of Wealth ("SOW") information remains outstanding;
- Enhanced Due Diligence ("EDD") requirements have not been completed; or
- previously submitted documentation is insufficient, expired, or cannot be verified.

Where CDD remains incomplete, the customer's account shall be referred for restriction.

SANCTIONS MATCH

Step 1 – Alert Generation

- A sanctions alert may be generated through:
- Customer onboarding;
- Ongoing customer screening;
- Periodic sanctions re-screening;
- Customer profile updates;

- Transaction monitoring;
 - Payment screening; or
 - Manual identification by an employee.
 - Upon generation of a sanctions alert, the customer's record shall automatically be referred to the Risk Team for review.
-

Step 2 – Initial Assessment

The Risk Team shall review the sanctions alert to determine whether the match is likely to represent:

- a False Positive; or
- a Potential True Match.
- The review shall consider, where available:
 - Full legal name;
 - Aliases;
 - Date of birth;
 - Nationality;
 - Country of residence;
 - Residential address;
 - Identification document details;
 - Passport or national identification number;
 - Other available identifying information.

Where additional information is required to determine whether the alert is genuine, the Compliance Team may request further documentation from the customer.

Step 3 – False Positive Review

Where the Risk Team determines that the sanctions alert is a false positive, the reviewer shall:

- document the rationale supporting the decision;
- retain supporting evidence;
- close the alert within the monitoring system; and
- continue the business relationship, provided no other compliance concerns exist.
- False positive determinations shall be sufficiently documented to demonstrate the basis upon which the alert was dismissed.

Step 4 – Potential or Confirmed Match

Where the Compliance Team cannot reasonably exclude a sanctions match, or believes the customer may be a designated person or entity, the matter shall immediately be escalated to the MLRO.

- Pending completion of the review, the Compliance Team shall implement appropriate account restrictions, which may include:
 - suspension of further deposits;
 - suspension of withdrawals;
 - suspension of gaming activity;
 - restriction of account access; and
 - any additional controls necessary to mitigate sanctions risk.
 - The level of restriction shall be proportionate to the nature of the identified sanctions risk and applicable legal requirements.
-

Step 5 – MLRO Assessment

- The MLRO shall independently assess the sanctions alert by reviewing:
 - the customer's complete profile;
 - screening results;
 - supporting documentation;
 - any additional information obtained;
 - the applicable sanctions designation; and
 - any relevant legal or regulatory obligations.
 - Where necessary, the MLRO may obtain additional information before reaching a final determination.
-

Step 6 – Outcome

- Following completion of the assessment, the MLRO shall determine whether:
- the alert represents a false positive;
- additional investigation is required;
- the customer relationship should be restricted or terminated;
- an internal report should be maintained; or
- any reporting or notification obligations apply under applicable sanctions legislation or regulatory requirements.
- The rationale supporting the decision shall be documented in the case management system.

TERMINATION DECISION

The Risk Team or MLRO shall consider termination of the business relationship where one or more of the following circumstances apply:

- the customer fails to complete Customer Due Diligence ("CDD") or Enhanced Due Diligence ("EDD") requirements within the prescribed timeframe;
- the Company is unable to satisfactorily verify the customer's identity;
- Source of Funds ("SOF") or Source of Wealth ("SOW") cannot be satisfactorily established;
- the customer refuses to provide information or documentation required to comply with AML/CFT obligations;
- the customer submits false, misleading, or fraudulent information or documentation;
- the customer is identified as a confirmed sanctions target or designated person;
- the customer presents an ML/TF/PF risk outside the Company's defined risk appetite;
- the customer is involved in suspected fraud, collusion, account sharing, chip dumping, value transfer, or other prohibited activity;
- suspicious activity remains unexplained following investigation;
- the customer breaches the Company's Terms and Conditions in a manner that creates an unacceptable AML/CFT risk; or
- the Company is otherwise unable to comply with applicable legal or regulatory obligations while maintaining the relationship.

RETURN OF CUSTOMER FUNDS

Step 1 – Determine Account Balance

The Compliance Team shall confirm:

- the available customer balance;
- pending wagers or unsettled bets;
- pending withdrawals;
- bonus balances or promotional credits;
- any administrative adjustments; and
- whether the available balance represents customer funds eligible for withdrawal.

Only cleared customer funds shall be considered for return.

Step 2 – AML Assessment

Before authorising the return of funds, the Compliance Team shall determine:

- the reason for account termination;
- whether Customer Due Diligence has been completed;
- whether an internal investigation remains ongoing;
- whether an Internal Unusual Activity Report has been submitted;
- whether the MLRO has identified reasonable grounds for suspicion;
- whether an external report has been submitted to the FIU Curaçao;
- whether sanctions restrictions apply; and

- whether any legal or regulatory restriction prevents the return of funds.

Where uncertainty exists, the matter shall be referred to the MLRO.

Step 3 – Determine Appropriate Action

Following the AML assessment, one of the following actions shall be taken.

Scenario 1 – No Suspicion Identified

Where:

- the relationship is terminated solely due to incomplete CDD or commercial reasons; and
- no suspicion of ML/TF/PF has been identified,

the Company may return the customer's available funds.

Where practicable, customer funds should be returned using the same verified payment method from which the original deposits were received.

Alternative payment methods shall only be used where appropriately verified and approved by the Risk Team.

Scenario 2 – Suspicion Exists

Where the MLRO has identified reasonable grounds to suspect ML/TF/PF, the return of customer funds shall not be processed until the MLRO has determined the appropriate course of action, taking into consideration:

- applicable AML/CFT legislation;
 - FIU Curaçao requirements;
 - instructions issued by competent authorities; and
 - the risk of prejudicing any investigation or committing a tipping-off offence.
-

Scenario 3 – Sanctions or Legal Restriction

Where the customer is identified as a sanctioned individual or where a competent authority has imposed restrictions on the account, customer funds shall not be released unless permitted under applicable law or authorised by the relevant competent authority.

MLRO Approval

The MLRO shall approve any decision to:

- withhold customer funds for AML/CFT reasons;
-

- delay the return of customer funds;
- refuse the return of customer funds; or
- depart from the standard return of funds process.

The rationale supporting the decision shall be fully documented.

Customer Communication

Where customer funds are returned, Customer Support shall communicate the outcome using approved communication templates.

Where the return of funds is delayed or refused due to AML/CFT considerations, communications shall be carefully managed to ensure that the customer is **not tipped off** regarding any internal investigation, suspicion, or external reporting.

VII. TRAINING

The Company shall implement and maintain effective measures to ensure that all Personnel are The Compliance Department shall develop and maintain an AML/CFT training programme appropriate to the Company's business model and ML/TF/PF risk profile.

Training topics shall include, where applicable:

- AML/CFT legal and regulatory obligations;
- the Company's AML/CFT Policy and Operational Manual;
- Customer Due Diligence ("CDD");
- Enhanced Due Diligence ("EDD");
- Source of Funds ("SOF") and Source of Wealth ("SOW");
- sanctions screening;
- Politically Exposed Persons ("PEPs");
- transaction monitoring;
- customer activity monitoring;
- Player-to-Player ("P2P") monitoring;
- unusual and suspicious activity indicators;
- internal reporting procedures;
- tipping-off prohibitions;
- record keeping obligations; and
- emerging ML/TF/PF typologies relevant to online gambling.

Training materials shall be reviewed periodically and updated to reflect regulatory changes, emerging risks, and lessons learned from internal compliance reviews.

INDUCTION TRAINING

All new employees whose roles involve customer interaction, transaction processing, compliance, fraud prevention, payments, or any other activities related to the Company's AML/CFT framework shall complete AML/CFT induction training as part of the onboarding process.

The induction training shall be completed **prior to, or as soon as reasonably practicable after, the employee commences duties** and before the employee is permitted to perform AML/CFT-related functions independently.

The induction training shall, at a minimum, cover:

- the Company's AML/CFT Policy and Operational Manual;
- individual AML/CFT roles and responsibilities;
- Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") procedures;
- customer identification and verification requirements;
- transaction monitoring and customer activity monitoring;
- identification and escalation of unusual or suspicious transactions and activities;
- internal reporting procedures;
- sanctions and Politically Exposed Person ("PEP") screening;
- tipping-off prohibitions; and
- record keeping obligations.

Upon completion of the induction training, the employee shall acknowledge their understanding of the Company's AML/CFT requirements and comply with all applicable policies and procedures. The Compliance Department shall maintain records of all induction training completed, including attendance, training materials, and assessment results where applicable.

ANNUAL REFRESHER

All relevant employees shall complete mandatory AML/CFT refresher training on an annual basis to ensure they remain informed of applicable legal and regulatory requirements, internal policies and procedures, emerging ML/TF/PF risks, and changes to the Company's products, services, or control framework.

The Compliance Department shall monitor completion of the annual refresher training and maintain appropriate training records, including attendance and assessment results where applicable.

VIII. RECORD KEEPING

The Company shall maintain and retain adequate records to demonstrate compliance with its Anti-Money Laundering and Counter-Financing of Terrorism ("AML/CFT") obligations and to enable the reconstruction of business relationships and activities where required.

Records shall be complete, accurate, and maintained in a manner that allows for their prompt retrieval without undue delay.

SCREENING RESULT

Upon completion of sanctions, Politically Exposed Person ("PEP"), and adverse media screening, the Compliance Team shall review and record the outcome of the screening within the customer management system with the officer's name, and date of the screening.

Each screening alert shall be assessed to determine whether it represents a false positive, a potential match, or a confirmed match requiring further investigation or escalation.

The outcome of the screening shall be recorded using one of the following classifications:

- **Cleared** – No matches or adverse information identified.
- **False Positive** – A potential match has been reviewed and determined not to relate to the customer. The rationale supporting the decision shall be documented.
- **Potential Match** – The screening result requires further investigation or additional information before a determination can be made.
- **Confirmed Match** – The customer has been confirmed as matching a sanctions list, PEP record, or adverse media result requiring escalation and appropriate action.

All screening results, supporting evidence, investigation notes, and decisions shall be retained within the customer record to ensure a complete audit trail and support regulatory review.

MONITORING RECORDS

The Compliance Team shall maintain complete and accurate records of all monitoring activities performed throughout the customer lifecycle to demonstrate compliance with the Company's AML/CFT obligations and to provide a clear audit trail of all reviews, investigations, and decisions.

Monitoring records shall be created and maintained for all transaction monitoring reviews, customer activity reviews, Player-to-Player ("P2P") monitoring, Customer Due Diligence ("CDD"), Enhanced Due Diligence ("EDD"), sanctions screening, Politically Exposed Person ("PEP") reviews, adverse media screening, and any other AML/CFT monitoring activities.

At a minimum, monitoring records shall include, where applicable:

- Date and time of the review;
- Customer Identification Number ("Customer ID");
- Type of monitoring activity or alert;
- Description of the trigger event or reason for the review;
- Summary of the review and investigation performed;
- Supporting information and documentation considered;
- Customer Risk Assessment updates, where applicable;
- Actions taken, including any account restrictions or additional due diligence measures;
- Escalation to the MLRO or Senior Management, where applicable;

- Final outcome and rationale; and
- Name of the Compliance Analyst or reviewer completing the review.

All monitoring records shall be maintained within the Company's case management or customer management system and shall be readily available for internal audit, regulatory inspection, and competent authority requests.

STR/SAR RECORDS

The Company shall maintain complete, accurate, and confidential records of all Internal Unusual Activity Reports ("IUARs"), Suspicious Transaction Reports ("STRs"), Suspicious Activity Reports ("SARs"), investigations, and related correspondence to demonstrate compliance with applicable AML/CFT obligations.

The MLRO shall be responsible for ensuring that all STR/SAR records are securely maintained and are accessible only to authorised personnel with a legitimate business need.

At a minimum, STR/SAR records shall include, where applicable:

- Internal Unusual Activity Reports ("IUARs");
- Supporting documentation and evidence reviewed during the investigation;
- Transaction and customer activity analysis;
- Customer Due Diligence ("CDD") and Enhanced Due Diligence ("EDD") records relevant to the investigation;
- Source of Funds ("SOF") and Source of Wealth ("SOW") information, where applicable;
- Sanctions, Politically Exposed Person ("PEP"), and adverse media screening results;
- MLRO investigation notes and assessment;
- Decisions, recommendations, and approvals relating to the investigation;
- Copies of any STRs or SARs submitted to the Financial Intelligence Unit ("FIU") Curaçao;
- Correspondence with the FIU or other competent authorities, where applicable; and
- The final outcome of the investigation, including any account restrictions, termination of the business relationship, or other remedial actions taken.

All STR/SAR records shall be maintained separately from the customer's general account records and treated as strictly confidential. Access shall be restricted to the MLRO, authorised Compliance personnel, Senior Management (where required), and competent authorities acting within their legal powers.

STR/SAR records shall be retained in accordance with the Company's Record Retention Procedure and applicable legal and regulatory requirements.

RETENTION PERIOD

The Company shall retain all records obtained for the purposes of Anti-Money Laundering and Counter-Financing of Terrorism ("AML/CFT") compliance for a minimum period of **five (5) years**.

The retention period shall commence from either the date on which the business relationship with the customer has ended; or the date of the occasional transaction, as applicable.

Where required by the Financial Intelligence Analysis Unit, the supervisory authority, or any competent law enforcement agency, the Company shall extend the retention period beyond five (5) years, provided that the total retention period shall not exceed **ten (10) years**, unless otherwise required by applicable law.

Where the Company ceases to carry out relevant financial business or activities, its record-keeping obligations shall continue to apply until the applicable retention periods have fully lapsed.

The Company shall also ensure compliance with any longer retention requirements arising under other applicable legal or regulatory frameworks, including data protection and corporate governance obligations.

Upon expiry of the applicable retention period, records shall be securely deleted or anonymised, unless further retention is required by law.

IX. REVIEW AND UPDATE

The Company shall ensure that its Anti-Money Laundering and Counter-Financing of Terrorism (“AML/CFT”) policies, procedures, and controls are subject to regular review and are kept up to date to ensure their ongoing effectiveness and compliance with applicable legal and regulatory requirements.

Such reviews shall take into account, at a minimum:

- changes in applicable laws, regulations, and regulatory guidance, including requirements issued by the Financial Intelligence Analysis Unit and other competent authorities;
- changes in the Company’s business model, products, services, delivery channels, customer base, and geographical exposure;
- findings arising from the Business Risk Assessment (“BRA”), Customer Risk Assessments (“CRA”), compliance monitoring activities, internal audits, and independent reviews; and
- emerging money laundering and terrorist financing (“ML/FT”) risks, trends, and typologies.

The AML/CFT framework shall be subject to a **formal review at least annually**, and more frequently where material changes, deficiencies, or elevated risks are identified.

Any proposed amendments to the AML/CFT framework shall:

- be appropriately documented, including the rationale for the changes;
- be reviewed and approved by the Board of Directors or an appropriately authorised body; and
- be communicated to relevant Personnel in a timely manner.

The Company shall ensure that updated policies and procedures are effectively implemented, and that relevant Personnel receive appropriate training or guidance in respect of any material changes.

ANNEX A- CUSTOMER REGISTRATION

Step 1 -Initial Registration

slot59.com/registration

look for... Q

Casino Sport

Begin your journey.

Telephone contact (International Format)

+351

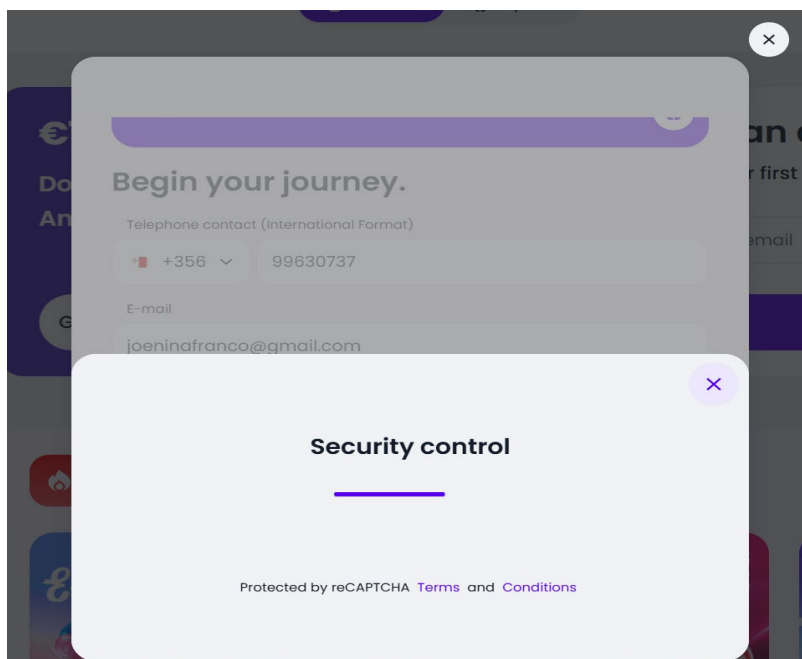
E-mail

Password

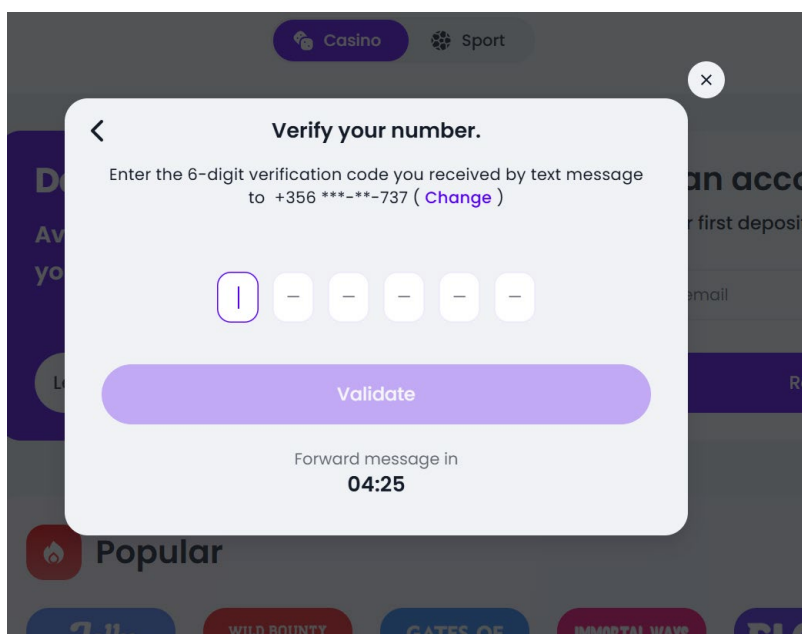
Promotional Code (if you have one)

Next

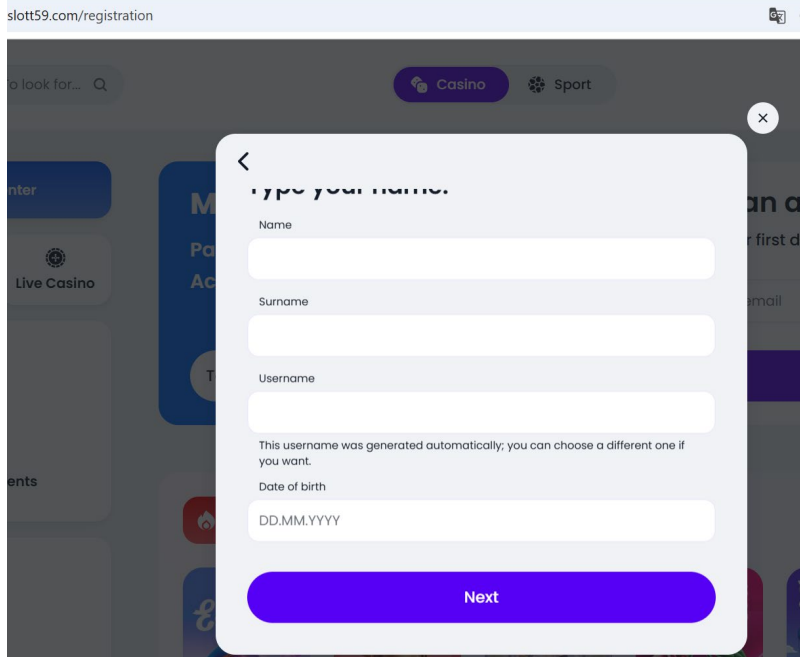
Step 2- System Validation



Step 3- Authentication



Step 3- Personal Information



Step 4- Age Validation

Name

Jo

Surname

Test

Username

JoTest-d

This username was generated automatically; you can choose a different one if you want.

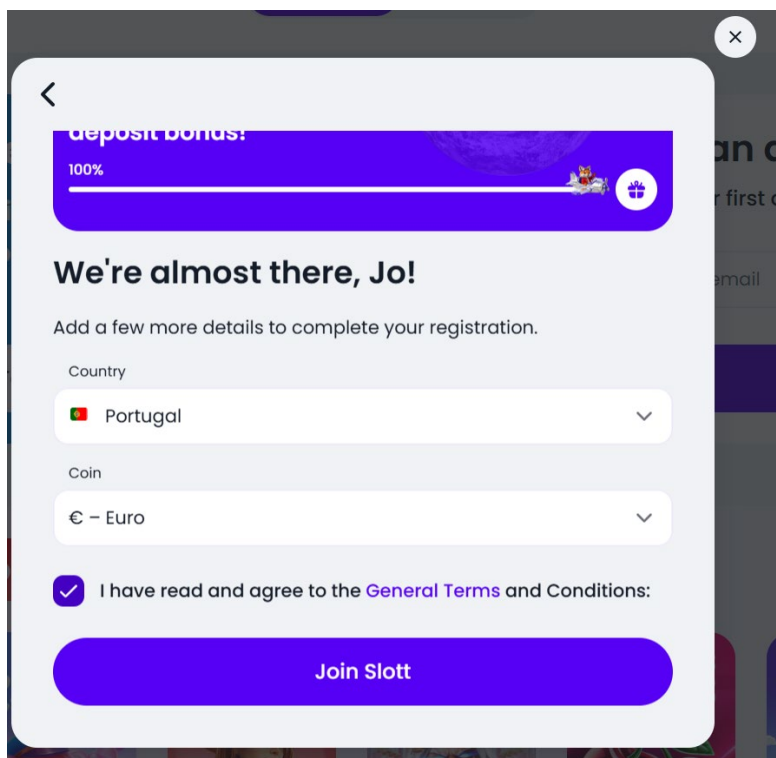
Date of birth

01.01.2010

You must be over 18 to play.

Next

Step 5- Terms and Conditions Acceptance



A registration completion modal for Slotit. At the top, a purple progress bar labeled 'deposit bonus:' shows 100% completion. Below this, the text 'We're almost there, Jo!' is displayed. A sub-header asks the user to 'Add a few more details to complete your registration.' There are two dropdown menus: 'Country' set to 'Portugal' and 'Coin' set to '€ – Euro'. A checkbox is checked, indicating agreement to the 'General Terms and Conditions'. A large purple button at the bottom is labeled 'Join Slott'.

<

deposit bonus:

100%

We're almost there, Jo!

Add a few more details to complete your registration.

Country

Portugal

Coin

€ – Euro

☒ I have read and agree to the [General Terms](#) and Conditions:

Join Slott

ANNEX B- ACCEPTABLE VERIFICATION DOCUMENTS

I. Identification

Document Type	Accepted	Requirements
Passport	✓	Must be valid, unexpired, clear, and contain a photograph, full name, date of birth, document number, and expiry date.
National Identity Card	✓	Government-issued, valid, unexpired, and contain a photograph.
Driver's Licence	✓	Government-issued, valid, unexpired, and accepted only where it includes a photograph and date of birth.
Residence Permit / Residence Card	✓	Accepted where issued by a government authority and includes a photograph and expiry date.

II. Address

Document Type	Accepted	Requirements
Utility Bill (Electricity, Water, Gas, Internet, Fixed Telephone)	✓	Must display the customer's name, residential address, and issue date. Mobile phone bills are generally not accepted.
Bank Statement	✓	Issued by a regulated financial institution and displaying the customer's name and address.
Credit Card Statement	✓	Issued by a regulated financial institution.
Government Correspondence	✓	Issued by a government department, tax authority, or social security authority.
Municipal or Local Authority Letter	✓	Showing the customer's residential address.
Residence Certificate	✓	Issued by the relevant government authority.
Tax Assessment or Tax Notice	✓	Issued by a competent tax authority.
Tenancy / Lease Agreement	✓	May be accepted where supported by additional verification where considered necessary.

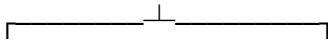
Sanctions Alert Generated

|



AML Review

|



|

|



False Positive Potential Match

|

|



Document Restrict Account

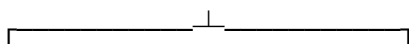
Close Alert

|



MLRO Assessment

|



False Positive Confirmed Match

|

|



Close Alert Terminate/Report (if required)