

KYC and AML Manual

Entertainment Art BV

Document Information:

Approval	Board of Directors
Responsible Office	Approving Official: Sandi Marinic Responsible Office: Payment risk and KYC department
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	May 31, 2025
Next Review Date	May 30, 2026

Version History:

Date	Version	Summary Changes	Approved by Management
April 10, 2025	1.0	Policy implementation	
May 31, 2025	1.1	Several Updates	

For any questions regarding this policy, please contact:

Name: Sandi Marinic

Phone: +52 1 55 2695 6963

Email: Sandi.marinic@ent-art.com


e-Management N.Y.
Managing Director

Contents

Contents.....	2
1. POLICY STATEMENT	3
1.1 PURPOSE.....	3
1.2 LEGISLATION FRAMEWORK.....	3
1.3 AUDIENCE	3
1.4 POLICY IMPLEMENTATION	4
2. CUSTOMER ACCEPTANCE POLICY	5
2.1 ENHANCED DUE DILIGENCE REQUIREMENTS AND PEPS	5
2.2 THE NATIONAL ORDINANCE ON IDENTIFICATION FOR FINANCIAL SERVICES OBLIGES US TO: 6	
2.3 THE NATIONAL ORDINANCE ON REPORTING UNUSUAL TRANSACTIONS IMPOSES THE FOLLOWING DUTIES:.....	6
2.4 BUSINESS RISK ASSESSMENT	6
2.5 CONTROL MEASURES	7
2.6 PROHIBITED ACCOUNTS	7
2.7 ONGOING MONITORING & REVIEW	7
3. THE ANTI-MONEY LAUNDERING REGULATIONS	8
3.1 ANTI-MONEY LAUNDERING COMPLIANCE OFFICER.....	8
4. PROCEDURES ON COMPANY PLATFORM.....	9
4.1 THE ENTERTAINMENT ART BV LICENSE AND OPERATOR SETS THE FOLLOWING MAIN RULES: 9	
5. REPORTING	12
5.1 INTERNAL COMMUNICATION.....	12
5.2 EXTERNAL COMMUNICATION	12
6. OUR KYC VERIFICATION FLOW.....	12
6.1 POLITICALLY EXPOSED PERSONS ("PEPs")	13
6.3 ENHANCED DUE DILIGENCE	13
6.4 ONGOING MONITORING.....	14
7. TRAINING & AWARENESS	14
8. SUPPLIER AND BUSINESS AFFILIATE DUE DILIGENCE	14
9. RECORD KEEPING	14
10. AUDIT & EVALUATION	14
Appendix I: Country Risk List	15
Appendix II: Business Affiliate and Supplier Due Diligence	15
Appendix III: Internal Unusual Activity Report Template	15

1. POLICY STATEMENT

ENTERTAINMENT ART BV, an exempted company incorporated with limited liability in the Curacao Island, (the "Company") is committed to the enforcement of laws to prevent money laundering, terrorist financing, proliferation and proliferation financing and other illegal transactions. It is the policy of the Company to ensure that high ethical standards are maintained and act in a manner that is in compliance with all laws, regulations, rules and regulatory statements of guidance and principles relevant to its business.

1.1 PURPOSE

The purpose of the AML manual is to map out the internal procedures and authorities that lead to the gaming entity complying with applicable Curaçao AML/CFT legislation. In the AML manual a translation is to be made from the legislation, which imposes general requirements and standards, to the how and by whom question in the context of the gaming operator itself.

1.2 LEGISLATION FRAMEWORK

The AML/CFT/CFP Regulations are aligned with the FATF Recommendations, alongside the various AML/CFT/ CFP legislations in Curacao, including:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- National Decree penalties and fines reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6.;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10 July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Ordinance of the 20th of December 2024 Containing Rules concerning Games of Chance (National Ordinance on Games of Chance) (PB 2024, no. 157);
- Curaçao Gaming Control Board Regulations for the combating of Money Laundering

1.3 AUDIENCE

The manual is applicable to all staff of the Company, inclusive of all officers, directors, managers, administrators and support staff and is not limited to individuals working under a contract of

employment but also includes temporary and contract staff. All relevant personnel must be aware of the existence and content of this manual, immediately bringing any anomalies or concerns to the attention of the Anti-Money Laundering Compliance Officer ("AMLCO") and/or Directors as appropriate.

1.4 POLICY IMPLEMENTATION

The Curaçao National Ordinance on identification when rendering services is the first pillar of Curaçao anti money laundering law. Online gambling is a relevant "service" under this law. A remote gambling operator is obliged under Article 1 paragraph b) 11) to identify and conduct customer due diligence on its players in accordance with this National Ordinance.

With the legislative changes of 2016, this law imposes significantly more obligations on service providers than "only" identification of their clients. Client research is required from the service providers specifically with a view to preventing money laundering or terrorist financing. Essentially the operator must have enough certainty that the person presenting him or herself to the operator as the player is indeed that person, that that person acts on his/her own account and that the funds used in the transaction are not proceeds of an illicit activity. In the context of online gambling this means that players can only be allowed to take part in the games after having at least filled out a form with their main identity features, such as full name, residential address, date and place of birth and nationality and type, issue date and number of an ID document.

The verification may, under the risk-based approach, be done in a later phase and may also be dependent on the amount deposited. Also, for the higher amounts of deposits, or the games that have a higher money laundering risk, the source of funds statement of a client's deposit should not only be on file but must actually be corroborated with evidence. Anonymous gambling is thus not allowed under Curaçao law and CIL license, however on low(er) risk wagers and clients part of the (full) due diligence verification, such as copy ID and source of funds scrutiny, may be postponed until a higher amount of deposits is reached. A threshold of not more than EUR 2,000 for identification verification and not more than EUR 5,000 for source of funds scrutiny is suggested. Actual thresholds may differ depending on the AML/ TF risk assessment made by the operator, considering the backgrounds and nationalities of clients, the sort of games and wagers offered, the financial instruments accepted, and other client due diligence measures taken etc. Such approach and the resulting internal policies, thresholds, procedures, roles and authorities must be laid down in an AML/CFT procedural handbook. This manual must be specific to the operations of the operator and refer to the Curaçao applicable rules.

Curaçao law leaves no room for the view that player identification or the verification of the account holder may later take place at pay-out and that the player's participation would therefore be subject to a customer due diligence still to be performed. When accepting a client, either or not using the risk-based approach and allowing him or her to play, the operator must be prepared to do the payouts in case the player wins.

2. CUSTOMER ACCEPTANCE POLICY

Customers are categorized based on risk levels: Low, Medium, High. Risk scoring includes geography, source of funds, transaction behavior, and client profile.

The Company does not accept anonymous accounts or clients from sanctioned jurisdictions.

IN ADDITION TO THE INITIAL ONBOARDING DUE DILIGENCE DESCRIBED ABOVE THE OPERATOR MUST CONTINUOUSLY scrutinize and monitor the players' activities during the relationship and conduct ongoing source or funds investigation. This client scrutiny may also be attuned to the risk sensitivity for AML / CFT of the wager, game or type of client. Depending on the risk profile of the client the operator is to review the client's file periodically and, in the case of sudden behavioral changes, (for instance, player starts to wager substantially more money or shifts from lower risk games such slots and roulette to poker etc.), the operator is to see into the backgrounds of these changes.

2.1 ENHANCED DUE DILIGENCE REQUIREMENTS AND PEPs

All PEP relationships require senior management approval prior to onboarding.

Not all situations where the law prescribes mandatory enhanced due diligence may be relevant to online gambling, but the operator may indeed find politically exposed persons amongst its clientele. It is compulsory to carry out client research to determine whether the player is PEP before onboarding. This is typically done by screening the client's name against a PEP's names database. All PEP relationships require senior management approval prior to onboarding. Access to these databases are commercially available.

In such circumstances it is mandatory that senior management of the operator agrees to accept this customer (not through an automated process) and it is mandatory to determine the source of the PEP's assets (source of wealth) and also the source of funds of the transaction at hand. After client acceptance the operator is to maintain a close monitoring of the PEP's betting transactions and financial instruments used to deposit and pay out.

We have developed internal anti-money laundering and deterrence of terrorism financing programs. This includes:

- Internal policies, procedures and controls, including employee screening
- a permanent AML/CFT training program for employees
- an audit function to test the systems in place.

Furthermore, we have an organizational unit that performs the compliance function in an independent and effective manner (a "Compliance Officer" or a "Money Laundering Reporting Officer"). This unit has the task of checking the company's compliance with the legal and internal rules and will typically also be the person or unit in charge with reporting unusual or suspicious transactions to the Curaçao Financial Intelligence Unit (FIU).

The National Ordinance on reporting unusual transactions to the Curaçao Financial Intelligence Unit (FIU) is the second pillar of Curaçao AML/CFT legislation. If in the course of the pre-acceptance due diligence a gaming operator is confronted with a transaction or an intended transaction initiated by a player that presents the possibility to be money laundering (or terrorism financing) related, we are under the obligation to report this (intended) transaction to FIU Curaçao.

2.2 THE NATIONAL ORDINANCE ON IDENTIFICATION FOR FINANCIAL SERVICES OBLIGES US TO:

- To identify their customers before performing a (gambling) service. This entails full name, home address, birth date and place of birth, nationality and number and issue date of ID document.
- To carry out a risk-based AML client assessment, including a source of funds verification.
- To refuse clients suspected or reasonably suspected of being involved in money laundering unwilling to identify or provide any other requested due diligence information.
- Ask clients whether they are PEPs, verify this and in such case perform 'enhanced due diligence' (mandatory AML high risk) with an emphasis on political corruption risk. All PEP relationships require senior management approval prior to onboarding.
- Prohibition of anonymous customers or customers with unclear source of funds.
- Measures to mitigate the risk of non-face-to-face business.
- Training program for personnel, to have an internal compliance function, and to have an external audit function.
- A five-year record keeping obligation for all client (player) transactions and client due diligence documentation collected (this may be extended on the instruction of FIU Curaçao).

2.3 THE NATIONAL ORDINANCE ON REPORTING UNUSUAL TRANSACTIONS IMPOSES THE FOLLOWING DUTIES:

- The obligation to register the entity with FIU Curaçao. FIU Curaçao then provides an online account that gives access to the portal where reports must be submitted.
- The obligation to immediately notify FIU Curaçao of all completed or intended transactions, which can be suspected to be related to money laundering or terrorism financing.
- The obligation to submit a report on all customers where the due diligence investigation (identification and further client due diligence) did not yield the desired result and, as a result, were refused as customers.
- The obligation to report all incoming (deposits) and outbound (pay-outs) transactions with customers of more than XCG 5,000 (±US\$ 2,700) to FIU Curaçao. This obligation exists regardless of whether there is any further reason to consider that transaction suspicious (it is a so called subjective mandatory indicator). It therefore can, and usually also will, concern a 100% legitimate transaction, which is still to be reported.

Our manual that is sufficiently Curaçao specific, it is, specific with reference to Curaçao laws and regulations and institutions. Our internal functions and roles will have to be identified and described, it will have to be clear who is doing what, who is overseeing who, who may have overridden or final decision powers and how the entire procedure is internally documented.

2.4 BUSINESS RISK ASSESSMENT

The purpose of the business risk assessment is to:

- Identify the key risks faced by the Company in its day-to-day operations;
- Assess the likelihood of each risk affecting the Company;
- Evaluate the procedures and controls in place to mitigate these risks.

From an AML perspective, the primary risk to the Company is that it enters a business relationship which results in the Company becoming involved in, or associated with, a financial crime. The potential negative impact of this risk is for both financially and operationally, and could result in reputational damage, loss of customers, regulatory actions and fines and lengthy legal proceedings.

2.5 CONTROL MEASURES

Managing and mitigating the risks will involve:

- Applying customer due diligence (CDD) measures to verify the identity of customers using the services of RapidID.
- Obtaining additional information or conducting enhanced due diligence on higher-risk customers via RapidID or by the Company directly
- Utilizing the services of RapidID and official national and international databases to screen all customers and relationship to ensure that they are not Politically Exposed Persons or subject to sanctions

In respect of risk from a money laundering or terrorist financing perspective, the Company operates in a very "HIGH" risk environment. And we are aware of this.

2.6 PROHIBITED ACCOUNTS

The Company prohibits opening or maintaining accounts for:

- Anonymous clients or shell banks
- Persons or entities from FATF-blacklisted jurisdictions
- Individuals under sanctions (e.g., OFAC, EU lists)

2.7 ONGOING MONITORING & REVIEW

All client accounts undergo periodic monitoring. High-risk clients are reviewed at least annually. Trigger events may prompt an interim review.

3. THE ANTI-MONEY LAUNDERING REGULATIONS

The Company requires all personnel to be aware of their personal anti-money laundering obligations under the legislation and regulation. All personnel should read and follow the procedures contained in this manual, as failure to maintain adequate awareness and adhere to procedures that are commensurate with an individual's position within the Company may result in internal disciplinary action, diminished compensation and/or termination of employment.

Money laundering is the process by which criminals seek to disguise the identity and true source of their illegal income and make it appear legitimate. Criminals launder money so they can avoid detection by law enforcement authorities and make personal use of illicit proceeds – including further criminal activity and investment in legitimate businesses.

The Anti-Money laundering Regulations (2020 Revision) ("AMLR") require anyone engaged in relevant business activities to have in place systems and training to detect and prevent money laundering.

In effect, the AMLR require the Company to:

- Maintain risk based, internal policies, procedures and controls. These procedures will include:
 - procedures for the determination of the true identity of the applicant for business;
 - procedures of internal control and communication as may be appropriate for the ongoing monitoring of business relationships or a one-off transaction;
 - procedures to assist in the recognition and reporting of suspicious activities;
 - the retention and maintenance of records for the prescribed period of time;
 - procedures to screen employees to ensure high standards of hiring;
 - adequate systems to identify risk as it relates to persons, countries and activities which must include checks against all applicable sanctions lists;
 - risk-management procedures concerning the conditions under which a customer may utilize the business relationship prior to verification.
- Appoint an Anti-Money Laundering Compliance Officer at management level with the responsibility for monitoring and ensuring internal compliance with the Laws
- Undertaking an Internal Audit Programme
- Ensure that there is a Staff AML training programme

The procedures contained in this manual satisfy the above requirements. They are also known collectively as Know Your Customer ("KYC") or Customer Due Diligence ("CDD") procedures.

3.1 ANTI-MONEY LAUNDERING COMPLIANCE OFFICER

In order to meet compliance requirements, set out in the AMLR, the Company has appointed an AntiMoney Laundering Compliance Officer ("AMLCO"). Senior management is responsible for the Company's global compliance program with all international and local legal and regulatory requirements applicable to the Company. Senior management is responsible for the oversight, selection and monitoring of the AMLCO. The Company relies on the AMLCO, under the supervision of senior management, for the following:

- Developing and maintaining systems and controls (including documented policies and procedures) in line with evolving requirements;
- Ensures regular audits of the AML/CFT programmes;
- Advises the Board of AML/CFT compliance issues that need to be brought to its attention;
- Reports periodically, as appropriate, to the Company's systems and controls.

At publication of this manual, the AMLCO is Sandi Marinic.

4. PROCEDURES ON COMPANY PLATFORM

How is fraud on company handled and detected? This document includes the overview of fraud system.

4.1 THE ENTERTAINMENT ART BV LICENSE AND OPERATOR SETS THE FOLLOWING MAIN RULES:

- Prohibition to offer wagers to players below 18 years of age, to Curaçao residents and to all personnel, including personnel of subcontractors.
- The license creates the legal fiction that, for the purposes of the wager, the player is deemed to have come to Curaçao in order to take part in the games.
- Back up resources in case of power failure must be in place.
- Staff and contractors involved must be of proper conduct, to be evidenced by being in possession of a (clean) police certificate.
- A personnel registry is to be maintained.
- All hardware and software must operate correctly and be tested regularly.
- A registry of hardware and software is to be maintained by the operator.
- All communication between player and operator is to be stored.
- Proper security and access authorization procedures must be implemented.
- Mandatory prior approval by the Ministry of Justice for types of wagers and games.
- The terms and conditions of the operator must be sufficiently clear to the player and must be approved by him/ her in order to take part.
- Anonymous playing is not allowed.
- Mandatory application of Curaçao law on the wagers (formation of a "gambling contract" by T&C acceptance under Curaçao law).
- Player to be given an identification number after acceptance of terms and conditions.
- Internal privacy and access policy on player data management.
- Each wager to have a maximum deposit and players only to take part once, or only to the maximum.
- Operator to make sure always to have enough funds to make payouts.

Objective

The objective of this document is to describe the Company fraud management system.

Scope

The scope of this document applies to the Company environment.

The standard AML requirements we are following during our everyday work:

- Follow AML compliance programs
- Due Diligence measures (CDD & EDD)
- Reporting
- Ongoing monitoring of customer activities
- Responsible Gambling
- Age verification
- SoF and SoW Screening in case of large or suspicious transactions and PEPs
All PEP relationships require senior management approval prior to onboarding.
- Payment Method Check

System based checks

Registration of players

The online registration process at our gambling Sites ensures that:

1. The player is at least 18 years old
2. The player has completed the registration form in its entirety
3. Players cannot register multiple times with the same data

Manual checks

Disabling Player's Deposits or Withdrawals

In case a notification from Payment Service Provider (PSP) or our Compliance Officer related to:

- chargeback
- unauthorized transactions
- other suspicious activities
- any other activity that could be related to fraudulent use of payment method account
- any activity regulated by Curacao Law and mentioned in this document

is received, specific payment method account (PMA) has to be frozen on player account, or all deposits disabled. KYC documents, including signed deposit authorization form for credit cards, have to be requested if not yet received. The same has to be done if any suspicious activity is noticed by the support operators.

Freezing of payment method account is currently possible for all integrated methods

One payment method account used by two or more players

Multiple payment method usage by two or more players is checked on three events:

- on withdrawal
- when player reaches pre-set system deposit limits
- routine transactions (deposits) checks

If a player uses someone else's payment method account, he/she is contacted via chat or e-mail and informed that the he/she shall only use credit cards and other financial instruments that lawfully belong to him/her. Players are asked to send their personal identification documents and an agreement signed by both parties for the consensual use of the payment method account.

Many payment method accounts used by one player

Usage of many payment method accounts by one player is checked on three events:

- on withdrawal
- when player reaches pre-set system deposit limits
- routine transactions (deposits) checks

Fraud Types

- High first deposits
High first deposit is considered to be one that is higher than the half of daily limit per risk profile of the player in question. Method of prevention: verification chat/ or email + verification via Payment Service Provider (PSP).
- Higher than usual deposits and sudden change in gaming pattern
Deposits three times higher than player's average without reason and sudden change in type of games played. Suspicion of loss of the account data. Prevention: email and/or chat verification
- Frequent deposits

Mostly within the first day of play, but further in player's age as well. Prevention: Limits are set per player's group, after reaching >> Email and/or chat verification

- High average bet on excluded games
High bet is considered over €20.00 or accordingly in other currencies on Table and Card games mostly. Alone this type doesn't say much, but mixed with any of other listed brings suspicion – acts in accordance with procedures
- Payment mixers (deposit-withdrawal)
In other words money laundering: depositing with one method (usually not the owner of one), mostly playing w/ bonus and withdrawing with couple of or none bets placed on another payment method. Prevention: withdrawals are made via the same method as initial deposits if relevant reason with according documentation wasn't given.
- Stolen/Suspicious details
- Players uses fake details in registration or gets access to someone's personal data and creates account using stolen details and CC. Prevention: fake details detected upon sign up and blocked accordingly (this is done on our side with Duplicate Check). In case of real, but stolen data, 3D gateway is the best prevention method for credit card transactions and notifications from PSP.
- Fraud rings
Group of people that have access to database or CC generator, creating multiple accounts in short period of time with similar patterns. Detected by the registration, gaming and communication patterns. Blocked upon recognition and blacklisted.
- Triangle country details mismatch
IPs of registered residency, actual location and credit card country mismatch. Detected upon registration and/or first attempted deposit. Blocked upon recognition if no relevant reason given supported by documentation.
- Bonus seekers
One person or group of people creating accounts with the sole purpose of attaining free bonuses. Recognized by the patterns and marked as bonus seekers, blocking the ability to receive any. In case of real bonus seekers (players depositing with payment methods with longer clearance period, receiving bonuses, withdrawing and never covering deposits), detected upon having more than 40% returned deposits.
- Name mismatch
Mismatch between player's name in the account and the name on the depositing CC is monitored with fraud rules. In case of a mismatch the deposit is not automatically credited to the player's balance but goes under review. The admin has the option to manually approve or decline the deposit.

5. REPORTING

5.1 INTERNAL COMMUNICATION

Chat operators and Shift managers are the first line of fraud detection using results from past knowledge as well as info from Fraud manager using tools from the BackOffice. Informing upon recognition Fraud manager who takes further actions and decisions.

5.2 EXTERNAL COMMUNICATION

PSP is always informed in cases of Credit Card fraud already done or intended. In larger scales, authorities could be notified as well.

Unusual transactions and all deposit transaction above 5.000 XCG are reported via MOT Portal Unusual Transaction Reporting Tool on website www.fiucuracao.cw

Reports

- Chargebacks (won and lost after representation) report done monthly, quarterly and yearly.
- Prevented Chargebacks report done monthly, quarterly and yearly.
- New fraud rings detected report done monthly, quarterly and yearly.

Reporting done to Head of Operation

6. OUR KYC VERIFICATION FLOW

The terms KYC and due diligence are used in relation to anti-money laundering, and both are used globally to describe customer identification and verification procedures, which comprise the obligations of Curacao financial services providers.

A general overview of the KYC due diligence requirements are set forth in this manual. In implementing the KYC requirements, we asked all our players to register on our site before onboarding and present all necessary information during Registration Process.

Knowing Your Customer ("KYC") is essential in the fight against money laundering. The Company should be satisfied that the Applicant for Business ("AFB") is who he or she claims to be as well as ensuring that sufficient information is gathered.

In order to set up a new customer account to purchase the Credits, a potential customer of our operation will be required to take the following steps to satisfy the Company's AML and KYC procedures:

- Obtain a certified copy of government issued photo identification and proof of address. If possible the original documentation should be sighted in a face-to-face meeting. These items can be in the form of a driver's license or passport as well as a utility bill, rental agreement, residential contract or government letter.
- Assign a risk level based on circumstance and hits on database screening.

As any problems encountered in relation to money laundering or criminal conduct are perhaps more likely to occur in the future when it might be difficult to remember what action was taken, it is essential that documentary evidence and records are properly maintained.

A High-Risk Customer will be one who presents a higher-than-normal adverse risk of involvement in money laundering or generates issues relating to money laundering requirements or any other matter that senior management or the AMLCO consider to be significant.

International best practice recommends that special attention should be applied to the following issues:

- High risk countries;
- Politically exposed persons ("PEPs"); All PEP relationships require senior management approval prior to onboarding.

- Businesses are attractive or susceptible to money laundering.

All High-Risk Relationships will be recorded for the purposes of reporting and monitoring.

6.1 POLITICALLY EXPOSED PERSONS ("PEPs")

All PEP relationships require senior management approval prior to onboarding.

A Politically Exposed Person or PEP is a term that is used to describe a person who holds a public position that may be exposed to corruption. The following list contains examples of persons who may be considered PEPs, although this list should not be viewed as exhaustive:

- Head of State;
- Government Ministers and Politicians;
- Influential public officials;
- Judges;
- Military commanders and high-ranking military officials;
- Family members or close associates of any of the above;
- Business partners or corporate connections of any of the above.

Adverse risk is created for PEPs as they might use their public position, or find that their public position is unknowingly used, for their own personal benefit or the benefit of others who may be involved in illegal activities such as corruption, bribery and fraud. All PEP relationships require senior management approval prior to onboarding. PEPs present considerable reputational risk to a financial service provider if that institution is found to be involved with public official who abuses his/her position. Adverse risk is increased considerably when a PEP is located in a high-risk country.

All PEP relationships require senior management approval prior to onboarding. The Company will ensure that each underlying customer is not a PEP by performing searches on official national and international databases to screen names against its database or referring to publicly available information. The results of such verification will be recorded. In the event that a PEP is identified, the Company will:

All PEP relationships require senior management approval prior to onboarding.

- Assign a rating of high risk to the customer;
- Complete PEP Report, ensuring Senior Management and the board of directors approves establishing a business with the customer;
- All PEP relationships require senior management approval prior to onboarding.
- Conduct enhanced due diligence and be vigilant in monitoring the business relationship;
- Ensure reasonable measures will be taken to establish source of wealth and source of funds;
- PEP relationships will be tracked in Viewpoint for the purposes of reporting and monitoring

All PEP relationships require senior management approval prior to onboarding.

6.3 ENHANCED DUE DILIGENCE

EDD will need to go beyond the normal requirements applied to the approval and monitoring of customers, as contained within this manual. EDD is an iterative, risk-based exercise - the higher the level of potential risk, the greater the corresponding level of due diligence.

For players that are residents of higher risk geographic areas, PEPs, high risk products/delivery channels, company is required to implement Enhanced Due Diligence measures. This would mean that players will be required to share proof of source of funds or wealth such as payslips, employment contracts, insurance payouts etc. Furthermore, in the event of a player being considered as subject to EDD, the first payment by means of withdrawal to the player to be subject to at least standard customer due diligence (regardless of the EUR 2,000 threshold).

All PEP relationships require senior management approval prior to onboarding.

6.4 ONGOING MONITORING

Once customer identification procedures are fulfilled and the customer is accepted, it will still be necessary to ensure that due diligence documentation continues to remain appropriate. In addition, it is essential to ensure that ongoing activity, if any, is consistent with the future plans and expectations that were advised at the outset of the relationship.

7. TRAINING & AWARENESS

AML TRAINING as part of the induction training, all new employees will receive anti-money laundering training. Permanent and temporary employees should be trained in the same way, while taking account the scope of work that might be allocated to a temporary employee.

New employees should be interviewed to ascertain the current level of understanding of money laundering. As a minimum, new employees should be provided with:

- Access to the Company's Anti-Money Laundering Compliance Manual;
- What is Fraud and types of Fraud
- How to Detect Fraud
- Payment Methods training

Annual AML training is mandatory for all employees. Participation is documented and effectiveness assessed

8. SUPPLIER AND BUSINESS AFFILIATE DUE DILIGENCE

Due diligence for third-party suppliers and affiliates includes:

- Collection of incorporation and ownership documents
- Valid license and AML Policy
- Background checks and sanction screenings

9. RECORD KEEPING

All records (KYC, transaction, internal reports) are retained for a minimum of 10 years in secure systems with restricted access.

10. AUDIT & EVALUATION

Internal audits are conducted annually. Scope includes transaction monitoring, onboarding compliance, recordkeeping, and reporting accuracy.

Appendix I: Country Risk List

High-risk: North Korea, Iran, Syria, FATF blacklist countries.

Low risk: Netherlands, Germany, Canada, Singapore.

Appendix II: Business Affiliate and Supplier Due Diligence

Documents required from partners:

- UBO Certificate
- Chamber extract
- Certified ID
- Proof of address
- AML Policy copy

Appendix III: Internal Unusual Activity Report Template

Report Date:

Client ID:

Transaction Details:

Narrative:

Filed By:

Follow-up Actions: