

**Anti-Money Laundering, Combating of
Terrorism and Combating of Proliferation of
weapons of mass destruction Policy
(AML/CFT/CFP Policy)**

CONFIDENTIAL

Prepared by	Date	Version
Rail Solutions Group B.V.	31 st October 2025	1.0 – Creation

Contents

1.	An Introduction to Anti-Money Laundering, Combating the Financing of Terrorism and combating the Proliferation of weapons of mass destruction (AML, CFT & CFP)	4
2.	How This Policy Works	4
3.	What is Money Laundering / Financing of Terrorism and Financing of Proliferation?	5
4.	Obligations of the Business.....	6
5.	When Could Our Employees Be Criminally Liable?	6
6.	'Tipping Off' or Prejudicing an Investigation.....	8
7.	Reporting Unusual or Suspicious Transaction	9
8.	Risk Based Approach.....	9
9.	Closing Accounts	10
10.	Overview of When We Carry Out CDD or EDD	11
11.	Initial Identification of Customers	11
12.	Verification of Identity	12
13.	Source of Funds.....	12
14.	Risk Indicators	13
15.	No Cash Policy and No Cheques or Bankers Drafts	14
16.	Payout Management / Withdrawal Process	14
17.	Training	15

Curaçao procedures

18.	Record Keeping	16
19.	Politically Exposed Persons (PEPs)	16
20.	Sanctions List	17
21.	Suspicious Transaction Reporting	18
21.1	Reporting Process	18
21.2	Suspicious Transaction Report	19

ABBREVIATIONS	
AML	Anti-money laundering
CDD	Customer Due Diligence
CFT	Countering the financing of terrorism
EDD	Enhanced Due Diligence
FIU	FIU Curacao
FATF	Financial Action Task Force
Guidance	AML-CFT Guidance for casino operators issued by Curacao Regulator
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
NOIS	National Ordinance Identification
NORUT	National Ordinance Reporting Unusual Transactions
PEP	Politically Exposed Person, family member of a PEP or known close associate of a PEP
PSP	Payment Services Provider
Regulator	Curacao Gaming Control Board
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
SOF	Source of Funds
SOW	Source of Wealth
The Regulations	NOIS and NORUT
UTR	Unusual Transaction Report

1. An Introduction to Anti-Money Laundering, Combating the Financing of Terrorism and combating the Proliferation of weapons of mass destruction (AML, CFT & CFP)

To combat money laundering (ML) and the financing of terrorism (FT), we are required to take steps to prevent and detect the use of any proceeds of crime, and to prevent and detect terrorist financing and proliferation of weapons of mass destruction (FP).

This policy sets out the information we will consider, and the steps we will take, to comply with our obligations in relation to AML, CFT and CFP.

We have appointed an MLRO, based on the Curacao legislation, who will work to implement and review our policies in this area. The MLRO will be responsible for receiving internal disclosures, deciding whether those disclosures should be reported to the relevant authorities, and making any necessary reports.

The MLRO is currently Bilal Bayrak

Any employee appointed to act as MLRO must be registered with the FIU. Any change in MLRO shall be notified to the FIU.

To ensure that our systems and controls are effective, we have identified a series of clear Risk Indicators which are proportionate to the risks faced by our business to deter possible money launderers from using our services, and/or to identify problem gamblers.

2. How This Policy Works

This document sets out the policies and procedures that must be followed by all staff employed by, or contracted to provide services to, **Rail Solutions Group B.V.** (the "Company").

These policies must be followed by all staff, whether on a full or part time basis, including management, officers, and directors to ensure that the Company successfully mitigates against the risk of the Company being used for money laundering and/or terrorist financing and adheres to its obligations under the relevant AML and CFT legislation.

The policies and procedures outlined in this document are mandatory to adhere to - there are no exceptions to this rule. All relevant staff must read this document, ensure that they understand it and any regulations and guidance issued from time to time by the regulator.

This is a 'live' document and will be reviewed and updated as and when necessary, based on business and/or regulatory changes. In any event, it will be reviewed at least once annually. Any updates and changes will then be communicated in writing to all stakeholders across the business via email and training shall be delivered to ensure that all relevant employees understand the changes and how they are to be implemented.

CONFIDENTIAL

3. What is Money Laundering / Financing of Terrorism and Financing of Proliferation?

To understand what is meant by money laundering, it is important to understand what is meant by the term 'proceeds of crime'.

The term 'proceeds of crime' refers to any money or other property which a person obtains (directly or indirectly) as a result of criminal activities (e.g., money from drug dealing, or stolen in a burglary or robbery, or stolen from an employer, or obtained through some fraudulent scheme, or any other form of 'ill-gotten gains').

If the person uses that money to acquire other assets, then those other assets are also the 'proceeds of crime' (e.g., if a person uses money earned from drug dealing to buy a car or a house, or spends money gained in a bank robbery to gamble, it must still be the 'proceeds of crime').

Money Laundering by a customer occurs either:

- (a) where he/she tries to spend the proceeds of crime on gambling (known as 'criminal spend'),
- or
- (b) where he/she is using our services to try to disguise the source of their money (i.e., 'classic' money laundering whereby a criminal tries to turn their ill-gotten gains into 'clean' money by 'layering' it through a series of otherwise respectable transactions, so that they appear to have derived their wealth from legitimate activities).

It is important to remember that simple 'criminal spend' on its own is enough to constitute money laundering (i.e. the use of criminal proceeds to fund gambling as a leisure activity), regardless of whether it is accompanied by any 'classic' money laundering activities. Spending that is inconsistent with an individual's apparent legitimate income may indicate that they are gambling with the 'proceeds of crime'.

Most of the people think that money laundering refers to funds acquired with drugs trafficking, but there are many predicate offences for money laundering such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes.

One of the most common forms of money laundering in the gambling sector is by problem gamblers who steal money (often from their employers) to fund their habit.

If we know or suspect that money laundering of any kind is taking place (whether it is 'criminal spend' or 'classic' money laundering), then we must report it accordingly.

If we know or suspect, or have reasonable grounds for knowing or suspecting, that a customer is engaged in money laundering, then we commit money laundering offences ourselves if we fail to report it appropriately. We can also commit money laundering offences if we assist customers to launder money, or if we 'tip off' customers that we are suspicious about their activities.

Similar principles apply if we know or suspect (or ought to suspect) that a customer is involved in financing terrorism. Terrorist financing is where money or property, either 'clean' or 'dirty' is intended to be used to fund terrorists or

Curaçao procedures

terrorist activity. Because it can include money which has come from a legitimate source, such as someone's wages or a charitable donation, it can be much harder to prevent or detect, as no crime has yet been committed.

Terrorist financing typically has a few more stages than money laundering. Although there is no formal structure, the key stages include:

- Making the money
- Gathering the money
- Moving the money
- Distributing the money
- Funding an action or event

The amounts of money involved in terrorist financing can be (but are not always) much lower than for money laundering.

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

Our AML, CFT and CFP obligations apply regardless of the amount of money involved (i.e., it is not necessary for the money involved to exceed a specified threshold).

Any employee who knows or suspects, or has reasonable grounds for knowing or suspecting, ML, FT or FP must report such knowledge or suspicion to our MLRO.

All employees should be aware that they may commit a criminal offence if they fail to escalate their suspicion of money laundering, terrorist financing or proliferation financing.

4. Obligations of the Business

Our business may also be subject to a wide range of regulatory and financial penalties if we fail to comply with our AML/CFT/CFP obligations. Our business may also be exposed to civil liability, and reputational and operational risk. When it comes to AML/CFT/CFP compliance, we therefore expect and encourage our employees to take their AML/CFT/CFP obligations very seriously.

5. When Could Our Employees Be Criminally Liable?

If you know, suspect or have reasonable grounds for knowing or suspecting that a customer (or another employee, or a B2B supplier, or any other person) is involved in money laundering or financing terrorism, including criminal spend, or attempting to launder money or finance terrorism you must escalate your suspicion.). A criminal offence is committed by you if you fail to report your knowledge or suspicion of money laundering or of providing financial assistance for terrorism, which you gain through your employment with us.

You must not allow a person whom you know or suspect to be involved in money laundering or of providing financial

CONFIDENTIAL

Curaçao procedures

assistance for terrorism to open an account with us or use an existing account with us. Otherwise, you may commit a criminal offence.

These Regulations, are the laws and decrees with regard to money laundering, financing of terrorism and financing of proliferation which must be covered in the company internal policies and procedures:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- 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 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 Decree for general measures, of the 10th of 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 10th of 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 Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

These laws and regulations and any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law form the main legal basis for the Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons.

6. 'Tipping Off' or Prejudicing an Investigation

Our MLRO will consider whether it is necessary to report suspicious activities to the relevant authorities. If a report is made to the authorities, it is important that the relevant customer is not 'tipped off' about the fact that they are under investigation. This could prejudice the ability of the authorities to investigate them. It is therefore vitally important that you do not disclose to a customer that you have suspicions about them which may result in a report being made.

You will commit an offence if you know or suspect that a disclosure of possible money laundering or of providing financial assistance for terrorism has been made by the MLRO to the relevant authorities, or that an investigation into money laundering is imminent or underway, and you disclose to any person not involved in the investigation - especially the customer(s) involved - that information (or any other matter that is likely to prejudice any such investigation).

However, it is still acceptable for you to make normal enquiries of a customer, conducted in a tactful manner, regarding the background of a transaction or activity that is inconsistent with the normal playing pattern of activity. We are required to make these enquiries, and simply making these enquiries in an ordinary manner should not give rise to the offence of tipping off or prejudicing an investigation. Indeed, such customer enquiries are likely to be necessary not only in relation to money laundering but also in connection with our responsible gambling duties.

You are unlikely to have actual knowledge or 'proof' that a customer is involved in criminal conduct. Therefore, you will rarely know for certain that the money flowing through the customer's account is the proceeds of crime. It is more likely that you will have a suspicion, from the customer's behavior or from the pattern of transactions in the account, that the customer may be involved in money laundering. If you have such a suspicion, then you must disclose it only to the MLRO (or DMLRO) immediately. And the same would apply if (somewhat unusually) you had actual knowledge or proof that a customer was involved in criminal conduct.

Escalate the issue as soon as it becomes apparent to minimize the risk of delay. If you are put under pressure by the customer to honor his/her request/s, or to explain delays, please escalate the issue for assistance, whilst taking great care to avoid making any statement that may constitute tipping off.

If in doubt, please consult the MLRO.

7. Reporting Unusual or Suspicious Transaction

All suspicious transactions and intended transactions that may be related to money laundering need to be reported.

Our staff are trained to monitor for signs that any person may be committing an offence.

Where there is a suspicion that an offence may be taking place, this will be reported to the FIU as soon as reasonably practicable. As mentioned in section 8, both unusual transactions (objective indicators) and suspicious transactions (subjective indicators) need to be reported to the FIU.

The following transactions or intended transactions are deemed unusual:

- a. Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b. Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c. Transactions in the amount of XCG 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means.

This includes but is not limited to:

1. A cashless transaction in the amount of XCG 5,000 or more.
2. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
3. Accepting or releasing a deposit in the amount of XCG 5,000 or more at the request of the client;
4. Sale to a customer of chips in the amount of XCG 5,000 or more. "Chips" include but is not limited to tokens and credits.
5. A cash out in the amount of XCG 5,000 or more;

Any transactions in the amount of EUR 2500 or more is deemed unusual transactions and directly reported to the FIU immediately as indicated above. The indicated examples are not limited, also credit card transactions and e-wallet transactions are to be reported to the FIU.

8. Risk Based Approach

We take a risk-based approach to our AML/CFT/CFP policies. The risk-based approach is applied when: (a) we identify the risks which are relevant to our particular business; (b) we design and implement our policies to manage and mitigate the identified risks; (c) we monitor and upgrade the way our policy operates in practice; and (d) we record the steps we have taken and why.

We also apply a risk-based approach to the ongoing monitoring of customer transactions. The risk-based analysis of our customers begins at the point when they initially register an account and deposit monies. It then continues throughout the life of the customer relationship, as we monitor their activity for signs of problematic behavior.

We have identified a series of clear Risk Indicators set out in section 14 below which are designed to identify possible changes in a customer's profile and behavior which represent an increased risk of problematic behavior. Where a customer is identified as representing a higher risk, then additional checks will be carried out. These additional checks may consist of enhanced verification of the customer's identity and/or taking reasonable steps to establish the customer's occupation, source of wealth and/or source of funds.

It is important for us to bear in mind that some risk indicators (for example, a pattern of increasing spend or spend inconsistent with apparent source of income) could be indicative of money laundering, but also equally of problem gambling, or both. There may also be patterns of play (for example, chasing losses) that appear to be indicative of problem gambling that could also be considered to indicate other risks (for example, spend that is inconsistent with the individual's apparent legitimate income could be the proceeds of crime). While patterns of play may be one indicator of risk, we must ask the necessary questions of customers when deciding whether to keep them as a customer or to terminate their account.

Where a customer appears to be high-risk (because they have triggered more Risk Indicators) then we must monitor them more closely. It is also important for us to monitor our customers' gambling activities across different products, so that we have a more complete picture of the risks posed by the activities of individual customers.

Throughout our relationship with each customer, we must monitor for signs that the customer is engaging in money laundering (including criminal spend); and we must consider whether there is a need to report suspicious activity.

9. Closing Accounts

Where, through their customer profile or known pattern of gambling activity, a customer appears to pose a risk of actual or potential money laundering, then we must monitor their gambling activity and consider whether further due diligence measures are required.

We will consider closing a customer's account in the following circumstances:

- where it is known that the customer is attempting to use our products/services to launder criminal proceeds or for criminal spend
- where the risk of breaches to AML obligations are considered by the MLRO to be too high
- where the customer's gambling activity leads to an increasing level of suspicion, or actual knowledge of, money laundering
- where the customer is proven to a reasonable degree of confidence to not be the identity they claim to be.

Additionally, where, in relation to any customer, we are unable successfully to apply CDD measures, we will consider closing the customer's account and the MLRO must submit a SAR to the FIU where they consider the circumstances to be suspicious.

We will, however, close the customer's account unconditionally if the requested information and documentation is

Curaçao procedures

not received within 30 days from the moment the customer engages in financial transactions equal to or more than EUR 2000, in order for us to complete CDD, and report the transaction to the FIU.

10. Overview of When We Carry Out CDD or EDD

Customer Due Diligence (CDD) involves identifying our customers, and then verifying their identity:

- the first stage of identifying our customers occurs when they register an account. All new customers are required to provide true and accurate personal details which include, amongst others, their full name, residential address, and date of birth. These details are used to establish the customer's identity.
- the second stage of verifying the identity of our customers involves carrying out checks to confirm that such a person exists at the address provided. An identity is verified by using documents or information obtained from a reliable source, independent of the person whose identity is being verified.

We use a third-party provider to screen customers against PEPs and Sanctions lists at signup state. If the player is identified as a PEP the account will be blocked, and any deposits refunded.

11. Initial Identification of Customers

When a customer opens an account with us, we need to check their identity. This is important for AML/CFT/CFP purposes (for example, to prevent a customer from opening multiple accounts without us knowing, or to enable us to link multiple accounts held by the same person). It is also important for other regulatory reasons (i.e. to enable us to comply with our age verification obligations, and to check whether the customer is subject to any self-exclusion arrangements).

Upon opening an account, all customers are required to enter the following details:

- Name
- Address
- Date of Birth
- Email address
- Telephone number
- Selected username and password
- Selected secret question and answer (to be used where a customer loses their login or password)
- Details of a payment card

If the customer is identified or suspected as underage, the Payments & Risk department will return the initial deposit back to the same payment method and block the account if necessary. All winnings will be retained by us.

12. Verification of Identity

We will verify the identity of the customer when the customer engages in financial transactions equal to or in excess of EUR 2000 by at least making reference to:

1. an unexpired government-issued ID document
2. proof of address document not to be more than 6 months old (if such a document indicated in 1 does not allow verification of the player's residential address)

We will verify the identity of the customer either electronically by making use of third-party providers or by making reference to documents.

The verification process will vary depending on whether we can verify the information provided using a third-party supplier or not.

There are 2 potential scenarios as follows:

1. Verification using a third-party supplier is not possible. This could be due to either of the following:
 - The jurisdiction from where the player is registering is not covered by the third-party provider.
 - Even though the jurisdiction from where the player is registering is covered by the third-party provider, the verification could not be made electronically.
2. Verification using a third party is possible and verification is made electronically.

When verification is not possible using a third party, the player is required to provide documents to verify their identity. Typical documents requested are a government issued ID, to verify identity and a utility bill or bank statement to verify address.

13. Source of Funds

The company scrutinizes Source of Funds information in certain higher risk situations. The following are such situations.

We conduct due diligence on a risk-based approach and will apply enhanced due diligence measures (EDD) and enhanced ongoing monitoring, in addition to our usual CDD measures, to manage and mitigate the money laundering or terrorist financing risks arising in the following cases:

- in any case where we identify, or information provided to us by the Regulator identifies, a high risk of

CONFIDENTIAL

money laundering or terrorist financing.

- in any case where we discover that a customer has provided false or stolen identification documentation or information and we propose to continue to deal with the customer.
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose.
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing

14. Risk Indicators

This section sets out how we use Risk Indicators to monitor the behavior patterns of our customers. These Risk Indicators *may* be signs that a customer is engaged in money laundering or problem gambling or both (or possibly neither) and may require further investigation or action by us.

There are four risk areas that the customer-specific risk assessment has to cover.

1. Customer risk, the risk of ML/TF that arises from maintaining relations with a given person. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth.
2. Geographical risk, the risk posed to the online casino by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. The online casino must have a list of countries that are considered as high risk and those that are considered low risk.
3. Product, service and transaction risk. Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others.
4. Distribution channels risk. The channels through which an online casino establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction

Higher risk customers will be subject to more frequent and deeper scrutiny than may be appropriate for lower risk customers.

The analysis which may be carried out is risk-based, and may include (but is not limited to): checking public databases (including bankruptcy searches, and press reports); asking direct or discreet questions about the customer's employment status, their financial background and source of wealth, source of funds, and carrying out a check of their property value etc.

15. No Cash Policy and No Cheques or Bankers Drafts

We do not accept cash deposits, and we do not process withdrawals in cash under any circumstances.

We do not accept deposits paid or made by cheque or banker's draft.

16. Payout Management / Withdrawal Process

The terms and conditions relating to the depositing and withdrawal of monies are clearly highlighted for customers as part of our Terms and Conditions. They are also clearly explained during the withdrawal process.

Withdrawal requests are reviewed and processed by the Anti-Fraud team at regular intervals each day. Under our Terms and Conditions, we reserve the right to request the customer to send us copies of documents to verify that they are the owner of any bank cards or other payment types which are being used to process deposits or withdrawals. Where we deem there to be a higher risk of fraud or money laundering, we reserve the right to require the customer to produce additional proof of identity and additional verification of their ownership of the method being used to withdraw funds.

If we receive notice of any chargeback, disputed deposit, or potential fraud, then the corresponding customer account will be frozen immediately. All reported chargebacks/fraudulent transactions will be investigated and challenged where possible and reported to the appropriate authorities.

Whenever possible we will remit the funds back to their original source.

Where a customer wishes to withdraw funds from their account, our systems will identify the following information:

- whether this is the first withdrawal request by a customer
- whether the withdrawal method is the same as that used to deposit
- whether the total value of refunds on the account is less than €2,000 (the amount is configurable depending on payment method and jurisdiction)

If a withdrawal request is made on an account which meets all the above criteria, the refund will be processed automatically (although our Anti-Fraud team is able to monitor withdrawals as they take place and make an immediate stop to the withdrawal if deemed necessary).

If a withdrawal request does not meet all the above criteria, then it will be reviewed by the Anti-Fraud team.

17. Training

Our MLRO is responsible for ensuring that all "relevant employees" are: (i) made aware of the law relating to money laundering and terrorist financing and to the requirements of data protection which are relevant to the implementation of the Regulations; and (ii) regularly given training in how to recognize and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing. It is important that all relevant employees understand the principles which underlie AML/CFT/CFP, so that they are able to apply and implement this policy correctly.

All relevant employees are required to undertake outsourced AML training and undertake outsourced refresher training annually. All relevant employees (including customer service staff) receive relevant AML/CFT/CFP training on induction and on an on-going basis. All relevant staff must undertake the AML/CFT/CFP training course within the first month of their employment.

This training is designed to ensure that staff react in an appropriate manner if and when cases of AML/CFT/CFP arise. Furthermore, all staff will be encouraged to use their judgment and report anything they consider suspicious to the MLRO.

Any employee who knows or suspects, or has reasonable grounds for knowing or suspecting, money laundering or terrorist financing must report such knowledge or suspicion to the MLRO. As part of training, all employees should be made aware that they may commit a criminal offence if they fail to make a report to the MLRO. All employees are advised to escalate the issue if they are in doubt about any case or incident.

Staff training will be delivered on a periodic basis (at least annually; and also upon joining for any new staff). Staff training is focused on the following topics: (a) an overview of the legal requirements in relation to combating money laundering and financing of terrorism; (b) a description of the process of money laundering, and how this could apply to our products and services; (c) an explanation of the AML policy we have adopted, including who to speak to for more information; (d) an overview of any changes in law or best practice since the last training session.

Where appropriate the MLRO will conduct spot tests and assessments to ensure that relevant staff are correctly applying our AML policy. The MLRO will report at least once a year to the board of directors on this subject.

A written record is kept of the training measures the business has taken and of the training given to relevant employees. The training records to be kept include: the name of the course/training module; the date on which such training has been delivered/received; who the training was delivered by; the names and job titles of the employees who received the training; and whether any subsequent tests (to evaluate the knowledge of the relevant employees) have been passed/failed and/or whether the training resulted in any relevant employees receiving any certification/qualification.

When new "relevant employees" are being recruited, we use appropriate employee screening processes to screen them to establish their integrity.

18. Record Keeping

In order to ensure the effectiveness of this policy, all relevant staff are required to keep records of the steps taken day-to-day in connection with this policy. This includes a record of the steps that have been taken, and the reasons why action has or has not been taken. These records can then be used to monitor and improve the effectiveness of our policy.

We are committed to complying with any investigations.

We keep the following records for at least 5 years following the closing of any customer account:

- details of all identity and age verification information obtained in relation to the customer;
- details of all payment methods used by the customer;
- details of all transactions by the customer, including full records of all gambling transactions (i.e. deposits, wagers, winnings and withdrawals); and
- copies of all SARs and other disclosure reports.

The MLRO is responsible for making this information available to the appropriate authorities on request.

In general, personal data relating to a customer will not be kept for any longer than 5 years from the date of the player's last transaction or when the account was closed. However, where suspicious activity was detected in relation to a particular customer, or a SAR was made, or the customer's account was closed by us due to AML/CFT/CFP concerns, then relevant personal data may be kept for such longer period as is regarded as appropriate in the circumstances.

19. Politically Exposed Persons (PEPs)

A "**politically exposed person**" (PEP) is someone who has been entrusted with a prominent public function, or an individual who is closely related to such a person. If we identify that a customer is a PEP, then that person will be in a higher risk category from an AML perspective; henceforth, the account will be blocked, and any deposits refunded.

A PEP is an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals:

- heads of state, heads of government, ministers and deputy or assistant ministers
- members of parliament or of similar legislative bodies
- members of the governing bodies of political parties
- members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are

CONFIDENTIAL

not subject to further appeal, except in exceptional circumstances.

- members of courts of auditors or of the boards of central banks
- ambassadors, chargés d'affaires and high-ranking officers in armed forces
- members of the administrative, management or supervisory bodies of state-owned enterprises
- directors, deputy directors and members of the board or equivalent function of an international organization.

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP

We use an external 3rd party provider to screen customers to see if they are PEPs. This check is triggered once customer's transaction reaches and/or exceeds EUR 2000 and also based on the risk level of the customer. If the player is identified as a PEP, the account will be blocked if deemed necessary after an internal risk assessment. In addition, we must be generally alert to situations which suggest that a customer is a PEP. These situations include:

- receiving funds from a government account
- correspondence on an official letterhead from the customer or a related person
- general conversation with the customer or related person linking the person to a PEP
- news reports suggesting that the customer is a PEP or is linked to one.

Should a customer be identified as a PEP, the account will be prompted for an internal risk assessment and reported to Senior Management.

20. Sanctions List

The purpose of imposing financial restrictions is to restrict access to finance by designated persons and to prevent the diversion of funds to terrorism and terrorist purposes. In all circumstances where an asset freeze is imposed, it is unlawful to make payments to, or allow payments to be made to, designated persons.

If a customer appears on a financial "sanctions" list, then we are prohibited from carrying out transactions with them. Financial sanctions apply to all transactions; there is no minimum monetary limit. We must carry out searches against the relevant lists to make sure that our customers are not on any relevant 'blacklists'.

If a customer is identified as a sanctioned individual, the account will be suspended and no deposits or gaming allowed.

If this is an existing customer, all funds in his/her wallet will be frozen. In every case, a report must be submitted to the MLRO, and a SAR will be submitted to the relevant agency.

21. Suspicious Transaction Reporting

The AML/CFT/CFP legislation requires our staff to escalate any suspicion of ML and TF.

Examples of suspicious activity could be:

- Transaction amount is substantially outside the normal pattern for the customer.
 - A request to make payments to a third party.
 - Failure to provide adequate identification documentation to satisfy identification/verification.
 - Large deposits followed by no/very few wagers being placed and in small amounts before withdrawals are requested.
 - Multiple accounts linked to one another.
 - Fraudulent identification documents or identification documents appear to have been tampered with or forged.

The examples above are non-exhaustive and you should exercise care and judgement in the course of carrying out your duties. A transaction that appears to be unusual is not necessarily suspicious. If you think a transaction is suspicious, you are not required to know the exact nature of the criminal offence or that particular funds are definitely those arising from the crime. It is not necessary to have evidence that money laundering is taking place to have suspicion. A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity to the MLRO then arises. Where in doubt whether a transaction is suspicious, escalate the issue.

Any suspicious transactions or activities **must be reported** by submitting an iSAR ticket or, alternatively, by emailing compliance@zenfinsin.com as soon as practicable following the process.

21.1 Reporting Process

The suspicious activity should only be discussed with the MLRO. Discussing the suspicion with anyone else could be construed as directly or indirectly “tipping off”, which is a **criminal offence**.

It is imperative that all relevant details are included and supporting documents enclosed. The reason for suspicion and the background to the suspicious transaction should be explained in detail.

The MLRO will acknowledge receipt and will review and investigate the suspicious activity as reported and will submit a SAR disclosure report to the relevant agency as soon as is practicable if appropriate.

YOU MUST NEVER DISCUSS YOUR KNOWLEDGE OR SUSPICION OR ANYTHING RELATED TO IT WITH THE RELEVANT PLAYER/INDIVIDUAL.

Any enquiry or communication from the relevant player/individual who is the subject of reporting/disclosure must be directed to compliance@zenginsin.com

21.2 Suspicious Transaction Report

The MLRO will determine whether the information gives grounds for knowledge or suspicion. If the MLRO determines that the information does give grounds for knowledge or suspicion, the MLRO must make a SAR report to the relevant agency as soon as is practicable.

No member of staff shall:

- disclose that they have made an internal disclosure to the MLRO if such disclosure is likely to prejudice any investigation that might be conducted following the disclosure.
- disclose that an investigation into allegations that an offence under the Regulations has been committed, is being contemplated or is being carried out where the disclosure is likely to prejudice the investigation.
- make any disclosure that is likely to prejudice an investigation where that person knows or suspects that an investigation is about to be conducted or falsify, conceal, or destroy or otherwise dispose of or cause or permit the falsification, concealment, destruction, or disposal of documents which are relevant to the investigation.
- tell a customer that a transaction is being delayed because an internal report has been generated and is pending assessment

The existence of a SAR shall not be disclosed to a customer at any time