

V 2.2

WINLINK B.V.

AML/CFT and CPF Manual

Anti-Money Laundering/Counter-Financing of Terrorism and
Proliferation of weapons of mass destruction Compliance.

Policy & Procedures Manual

Document / Revision History

Document Reference: WINLINK B.V. AML/CFT and CPF Manual Revision Number: 2.2 Total Pages: 42 Original issue date: 2023 Revision date: March 2025 Effective Date: June 2025	AML/CFT and CPF Policies and Procedures Manual								
<table><tr><td data-bbox="113 560 399 672">Written by:</td><td data-bbox="399 560 1511 672">Kristian Spasov</td></tr><tr><td colspan="2" data-bbox="113 672 399 983"></td></tr><tr><td data-bbox="113 672 399 983">Approved by:</td><td data-bbox="399 672 1511 983"><table><tr><td data-bbox="399 672 1133 983">Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V.</td><td data-bbox="1133 672 1511 983">Date: 27 June 2025</td></tr></table></td></tr></table>		Written by:	Kristian Spasov			Approved by:	<table><tr><td data-bbox="399 672 1133 983">Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V.</td><td data-bbox="1133 672 1511 983">Date: 27 June 2025</td></tr></table>	Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V.	Date: 27 June 2025
Written by:	Kristian Spasov								
Approved by:	<table><tr><td data-bbox="399 672 1133 983">Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V.</td><td data-bbox="1133 672 1511 983">Date: 27 June 2025</td></tr></table>	Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V.	Date: 27 June 2025						
Gouloud Mercedes Hammoud obo Global Related Services B.V. Managing Director WINLINK B.V.	Date: 27 June 2025								

Revision #	Version Date	Description of Changes
1.0	2023	Initial Draft
2.0	July 2024	Updated and extended: transaction thresholds, identification procedures, customer risk assessment, prohibited countries Added: risk score, customer acceptance policy <i>All changes are created and applied according to the regulations:</i> - Amendment to NOIS No. 92 and NORUT No. 99, as of May 16, 2024 - FATF Recommendations 2012, Updated November 2023 - AML/CFT/ CPF, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction I May 2024
2.1	October 2024	Updated and extended: applicable legislation, customer due diligence requirements in line with the Regulations of the Gaming Control Board.
2.2	March 2025	Updated and extended: transaction definitions, CDD scope (including retroactive checks and integrated PEP/sanction screening), threshold-based restrictions (Naf. 4,000 and 5,000), demo account procedures, foreign document guidance, ID expiry tracking, MLRO responsibilities, and prohibited countries list.

Context

Introduction.....	6
1. General Definitions.....	6
1.1 Stages of money laundering:	7
1.2 Combating Terrorist Financing and Weapons Mass Destruction.....	7
1.3 Responsibilities	8
1.4. Applicable Legal Framework.....	8
2. Prevention of Money Laundering and Terrorism Financing.....	9
2.1 Responsibilities of Senior Management	9
2.2 Implement and clearly communicate policies and procedures to staff.....	9
3.0 The Risk Based Approach	10
3.1 Identification of Risks	10
3.2 The Five Risk Pillars and Assessment.....	11
3.2.1 Monitoring of Risk	13
3.2.3 Supervision of the Implementation of the RBA.....	13
3.3 Implementation of the Risk Based Approach	13
3.4 The company's residual risk	13
3.5 Dynamic Risk Management	13
3.6 Ongoing Risk Assessment – Advanced	14
3.7 Customer Risk Profile	14
4. Customer Acceptance Policy	16
4.1 Failure or refusal to submit information	16
4.2 General Principles of the CAP	16
4.3 The Criteria in the Customer Risk Level Breakdown.....	17
4.3.1 Low Risk Clients	17
4.3.2 Medium Risk Clients	17
4.3.3 High Risk Clients	18
4.3.4 Extreme Risk	18
4.3.5 PEPs	18
5. Customer Due Diligence	18
5.1 Simplified due diligence.....	18
5.2 Customer due diligence	19
5.3 Enhanced due diligence.....	20
5.4 Registration Procedure.....	20
5.5 Sanction list Screening:.....	22
5.6 Player Verification Procedure.....	22
5.7 Minor Prevention Procedures	23



5.8 Politically Exposed Persons:	24
5.8.1 The meaning of a 'Politically Exposed Persons':.....	24
5.8.2 Measures Applied to PEPs	24
6. Record Keeping and Monitoring	26
6.1 General	26
6.2 Format of Records	26
7.0 On-going Monitoring Process	26
7.1 General Provisions of On-going Monitoring Process	26
7.2 Procedures of On-going Monitoring Procedures.....	26
7.3 Timeframes.....	27
7.4 Pay-out Management Procedure	27
7.4.1 Risk Profile for Winlink B.V.	28
7.5 Accounts accessed through VPN	28
8. Unusual Activity/Transaction Reporting.....	29
8.1 Knowledge.....	30
8.2 Unusual Transactions	30
8.3 MLRO's Report to the FIU.....	31
8.4 Submission of Information to the FIU.....	31
8.5 Duties and Responsibilities of the Money Laundering Reporting Officer (MLRO).....	32
9. Training.....	33
9.1 Employees' obligations.....	33
9.2 Employees' Education and Training.....	34
9.3 MLRO Education and Training Program	34
10. Independent Audit Function.....	34
11. Appendices	36
11.1 Appendix A I Suspicious Activity Report	36
11.2. Appendix B Prohibited countries	37
12. Senior Management Approval.....	42

Introduction

The AML/CFT policy document shall indicate and define the company's policies and procedures in place intended to prevent its products and/or services being used for ML/TF purposes. This document shall set the standard to be followed by the company, its officers and employees, the measures and controls in place and the internal practices to follow. The AML Policies and Procedures shall be reviewed at least on a yearly basis to determine if any updates and/or amendments are required. The frequency of such updates can be less should there be any regulatory change or change in the policies and procedures to be applied due to any change in the risks faced by the company or due to any changes in the assessment of certain risk factors arising out of publications made by the FATF, FIU and/or GCB.

Any updates and/or changes made to this document shall be presented to the board of directors who shall review and approved such changes.

1. General Definitions

For the purposes of this AML Policies and Procedures, unless the context shall prescribe otherwise:

"Business Relationship" means a business, professional or commercial relationship which is connected with the professional services offered by the subject person and which was expected, at the time when the contact was established, to have an element of duration.

"SDD" - simplified due diligence

"CDD" – customer due diligence

"EDD" – enhanced due diligence

"Gaming Company" means Winlink B.V. which is duly constituted company under the Laws of Curacao and its related companies and entities.

"Law" means any Laws and Acts legally enacted from time to time in Curacao, or which are applicable and enforceable in Curacao.

"AML Policies and Procedures" means the subject person's Risk Management & Procedures (this document) which has been drafted and adopted according to the Curacao Laws.

"Money Laundering and Terrorist Financing" means the money laundering offences and terrorist financing offences defined in the Law.

"Player/Client/Customer" means a natural person aiming to conduct a Business Relationship or conduct a single transaction with the company

"Politically Exposed Persons (PEPs)" means the natural persons who are or have been entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons.

"FIU" means the Financial Intelligence Unit of Curacao.

"KYC" abbreviation for Know Your Customer.

"GCB" means Gaming Control Board.

"CGA" means Curacao Gaming Authority.

"Transaction (Financial transaction)" means any deposit or withdrawal made to or from a player's account. This excludes bonuses. Amounts wagered and winnings are considered gambling transactions and are not classified as financial transactions.

“Occasional transaction” means a transaction with a registered one-off customer, who at that point is not expected to return or establish an ongoing relationship.

1.1 Stages of money laundering:

The company strives to ensure that all possible efforts are undertaken to prevent money laundering or the funding of terrorism and Proliferation of weapons of mass destruction and actively act to curtail such illicit activity. The company complies with the NOIS and NORUT, the GCB Regulations, the EU Fifth directive, FATF Recommendations and any other applicable laws and regulations.

Money laundering is an offence by which money derived from criminal activity is passed through a series of processes to disguise the ownership and management of such revenue which therefore cannot be traced back to the underlying crime. The process of money laundering makes such funds appear to have been generated from legitimate sources of business.

The stages of money laundering are as follows:

- I. Placement
- II. Layering
- III. Integration

Placement

Placement is the stage where the money is introduced into the financial system, the funds at this stage are still illegitimate and the launderer will try to incorporate and place the money derived from illicit activity into the system to start the process of money laundering. At this stage it is very important to understand where the money originates from, as the person with the intention of committing such act will need to obfuscate any link of the funds with criminal activity without attracting any attention.

Layering

At this stage the funds have managed to be deposited in the financial institution it is at this point layering is used through complex structures directed to lose all trace of the money and remove any trace of its origination from the proceeds of a crime. This may happen by conducting transactions to different jurisdictions. This process is intended to ensure that the funds are as far removed as possible from the proceeds of a crime.

It is important to prevent such an event by transaction by ensuring staff are equipped to ask the right questions whilst avoiding alerting the customer of any suspicion.

Integration

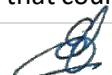
At this stage, the money derived from criminal activity has been made legitimate and placed once again into the financial system as legitimate funds. At this stage, the launderer has been successful in laundering the funds.

1.2 Combating Terrorist Financing and Weapons Mass Destruction

The intent and scope of such acts vary and differ from case to case, but the process used for the funding of terrorism can be quite similar to those methods used for money laundering.

Current legislation enforces Customer Due Diligence on transactions, and having this process in place has made such activity harder for those intent on laundering money generated from illegal activities. It is of utmost importance to the company that the policies and procedures are structured in a way that ensures compliance with regulators and legal frameworks, ensuring that the company is not an attractive vehicle for the purpose of terrorist financing.

The subject person's AML policies, procedures, and internal controls are designed to ensure compliance with all applicable legislation and best practice procedures. The policy is reviewed and updated regularly to ensure all applicable procedures and internal controls are up to date, accounting for both regulatory changes and internal changes that could



present new risk factors

1.3 Responsibilities

The Financial Department Management and staff are responsible for monitoring all transactions to and from the company and verifying the identity of all online registered players requesting a withdrawal or reaching any of the transaction thresholds. They must also establish parameters by which any suspicious activity can be immediately noted, and form procedures by which to solve these issues while keeping the risk to a minimum. The verification process will be documented in such a way that every player will have a profile and if any Unusual Transaction Report needs to be filed, all evidence in respect of the player will be in hand.

The following departments are directly targeted by the requirements of this procedure:

- Board of Directors – Approval and Signature requirements, especially in high risk scenarios,
Client Support (L1) – Understanding reporting requirements,
KYC (Risk) Department – Understanding and applying DD requirements, the difference between a fraud case and an ML case,
- Finance – Understanding the risks posed by ML/TF, the difference between a fraud case and an ML case,
- Compliance Officer – Ensuring all legislation requirements are met,
- MLRO – Updating Policy and ensuring all relevant employees are aware of AML requirements.

The scope of this procedure may be extended to other departments if the need ever arises, and all employees need to be attentive and aware of the information flow regarding prevention of ML and TF

1.4. Applicable Legal Framework

The Company has developed the current AML Manual in accordance with the applicable legislation of Curaçao, aligned with the Recommendations of the Financial Action Task Force and international standards of money laundering prevention, in particular (but not limited to):

- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- 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);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th 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 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 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);

- 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 (N.G. 2018, no. 34);
- National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
- National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
- National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update May 2024.
- Curacao Gaming Control Board, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.
- National Ordinance on Games of Chance (LOK, P.B. 2024, no. 157)

The Company performs regular monitoring for amendments to all Decrees and Regulations and updates the policies and procedures accordingly to meet any such changes. Besides these regulatory authorities, the Company also continually observes relevant international standards such as the recommendations of the Financial Action Task Force on Money Laundering ('FATF'), the Caribbean Financial Action Taskforce (CFATF) and the Guidelines and instructions of the European Commission as well as the six Directives of the European Union on AML and CFT.

2. Prevention of Money Laundering and Terrorism Financing

2.1 Responsibilities of Senior Management

As an online gaming operator management as well as the shareholder/s of the company understand and are aware that there is susceptibility to a certain level of ML/FT&PF risk. Management must stimulate awareness to detect the lack of implementation of stringent measures in order to detect fraudulent activity as the sites may become an easy target to launder money. The Winlink B.V. declares zero tolerance for ML/FT&PF and towards employees, players, partners who are engaged into ML/FT&CPF.

Senior Management of Winlink B.V. is aware of the stages of money laundering and ensure to take all preventative measures to combat, prevent and detect money laundering. Prevention is ensured by carrying out the following measures:

- Implement policies and procedures throughout the group of companies.
- Clearly communicate such policies and procedures to staff.
- Adopt a risk-based approach.
- Internal Controls.
- Customer due diligence procedures.
- Record keeping and Monitoring.
- Unusual activity reporting.
- Training.

2.2 Implement and clearly communicate policies and procedures to staff

Due to the size of the operation, management is principally responsible for most functions within the company. Management is aware of the policies and procedures in place throughout the group of companies. For example: withdrawals can be requested for amounts that have been turned over at least once. This protects the operator from being abused for money laundering purposes and protects our system from free-of-charge deposits that may be abused to our disadvantage. All withdrawal requests are initially checked by management, which monitors all the withdrawal

requests and denotes those which are suspicious, based on any suspected fraudulent background. Due the size of the operation and knowledge of the player database, various customer/s due diligence and verification processes are carried out manually by management. In any case where a transaction is complex or unusually large or there is an unusual pattern of transactions and the transaction has no apparent economic purpose in relation to the nature of the business, such transaction is flagged manually as suspicious, and investigations are immediately kicked off.

Checks for multiple accounts, individuals which may have been blacklisted by any relevant organization or company, transaction, and betting behaviour, handled amounts, deposit/withdrawal methods are carried out in order to identify any suspicious activity.

3.0 The Risk Based Approach

The AML Regulations imposes prevention and enforcement for subject persons. Therefore, Winlink B.V. applies the risk-based approach for the purposes of preventing and detecting fraud.

3.1 Identification of Risks

The following steps are followed to implement the risk-based approach:

Identification Process: Identify internal and external risk factors that increase the risks faced by the company. Winlink B.V. must assess both domestic and foreign money laundering risks affecting their target markets.

Non-Compliant Countries: If players register from countries that are non-compliant with AML regulations and fraud management procedures, the operator must ensure that all players adhere to the company's procedures. Registrants are from reputable jurisdictions, reducing the risk of non-compliance due to unimplemented regulations.

Business Risk Assessment: To stay aware of and address risks, the company must update its business risk assessment annually or as needed. This ensures the company remains aware of changing risk scenarios and can mitigate them effectively.

3.2 The Five Risk Pillars and Assessment

The Company calculates the risk score of players to ensure that the Client does not pose a high risk of money laundering or funding of terrorism. This assessment is based on five main categories, each incorporating specific factors:

a) Customer Risk – customer`s background.

Customer Risk	Description and Risk Level
If the customer is under the sanction	YES - EXTREME NO - LOW
If the customer is a PEP	YES – EXTREME NO- LOW
Customer`s Source of Wealth Explained	● Extreme: - Source of Wealth unverified, - False declarations made, - Generated from a sanctioned country. ● High: - Have multiple sources of income(more than 3), - Gifts/Donations, - Income generated from VFA(non-regulated) ● Medium: - Actual/Punitive damages awarded as a result of litigation (court of settlements), - Selling of Real Estate, - Profits and Dividends from a financial
	investment, - Investment of Private Securities, - Income generated from VFA(regulated) ● Low: - Employment, - Inheritance, - Winnings from a licensed entity, - Investment in Publicly Listed Securities, - Royalties, - Rental Income,
Duration of customer relationship	Less than 3 months- High 3 to 12 months – Medium More than 1 year - Low
Estimated Average bet size(per month)	0,00 - 10,00 USD – Low 11,00 – 50,00 USD – Medium 51,00 + USD - High
Multiple casino accounts or wallets	- YES – HIGH - NO – LOW

b) Jurisdiction Risk - the countries or geographic areas in which it operates.

This risk factor is based on the jurisdiction risk analysis, which is presented in a separate document and can be accessed upon request.

The jurisdiction risk assessment is based on the following player data: residential Address, nationality, place of birth, IP address.



c) Product Risk - products and services.

TYPE OF GAME	Description and Risk Level
Sportsbook	HIGH
Virtual Sports	MEDIUM
E-Sports	HIGH
Casino – Slot Games	LOW
P2P – Casino	HIGH
Live Casino – vs House	MEDIUM

d) Transaction Risk - type, volume, method by which transactions are carried out.

Transaction Type	Description and Risk Level
Deposit/withdrawal method	● High: -Cash - Prepaid card / vouchers - VFAS (CRYPTO CURRENCIES) - Online E-Wallets or all PSPs that allow customers to fund with cashor quasi-cash - third-party accounts or cards -Transfer of funds between gaming accounts -Use of casino accounts (Withdrawal without Play) ● Medium: - Credit Card EU/EEA/SEPA/Visa/MasterCard - Online E-Wallets or all PSPs WHICH DO NOT ALLOW CUSTOMER TO FUND WITH CASHOR QUASI CASH ● Low: - Debit Card EU/EEA/SEPA/Visa/MasterCard - Digital Wallets (Apple/Google/Samsung pay)
Withdrawal amount (perrequest)	\$0-\$2199 (Low) \$2200-\$9999 (Medium) \$10000 (High)
Deposit amount (per session)	\$0-\$2199 (Low) \$2200-\$9999 (Medium) \$10000+ (High)

e) Interface Risk - delivery channels. The way in which business relationships are established and maintained.

Risk Type	Description and Risk Level
Client interaction interface	NON-FACE-TO-FACE THROUGH AGENT (High)
	NON-FACE TO FACE – VPN (High)
	NON-FACE-TO-FACE THROUGH INTERMEDIARY (High)
	NON-FACE-TO-FACE THROUGH INTRODUCER/AFFILIATE (Medium)
	NON-FACE TO FACE DIRECTLY (Medium)

In all risk sections, if one or more extremes are present, the whole section will be classified as extreme and senior management will be contacted before proceeding any further.

The information in section 3.2 is based on a separate document Risk Score and can be accessed upon request.

3.2.1 Monitoring of Risk

Management scrutinizes risk assessments carried out in order to recognize gaps in procedures and areas of improvement in procedures to reduce inefficiencies. It is important to note that inefficiencies may be present in both procedures and lack of technical expertise adopted by staff.

3.2.3 Supervision of the Implementation of the RBA

This process includes the review of risk assessments reviewed and the due diligence collected especially on high-risk players.

3.3 Implementation of the Risk Based Approach

Following the identification of inherent risk, management is required to implement the respective controls in order to mitigate such risks. The first step to adopting some form of internal control, the company must appoint at least one individual (depending on the size of the company) for the compliance with these Regulations. Independent testing should be conducted to confirm that the controls are effective and do not create new risks. Management also ensures that staff are trained to apply any updates in regulations.

3.4 The company's residual risk

Taking into consideration the assessed risks, the company shall determine the type and extent of measures it will adopt to manage and mitigate the identified risks in a cost-effective manner. This document will provide a brief description of the procedures to be adopted by the company such as SDD, CDD and EDD, the type and quality of documents to be obtained, ongoing monitoring of clients, identification and verifications policies and procedures, identification, and verification of source of wealth and source of funds amongst others.

3.5 Dynamic Risk Management

Risk management is a continuous process, carried out on a dynamic basis. Risk assessment is not an isolated event of a limited duration. Clients' activities and requests change as well as the services they require to be provided with.

In this respect, it is the duty of the MLRO to undertake regular reviews of the characteristics of existing and new Clients, services and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented as per the requirements described herein, as applicable.

It is also important for the MLRO to monitor and ensure that the proper procedures are being implemented, and the risk-based approach principle is truly being followed in all areas of the subject person. By doing so, one will also be



ensuring that although certain products/services or clients may be of a higher risk, the company may continue providing these services and assisting these clients due to the risk being mitigated through the proper policies being implemented.

3.6 Ongoing Risk Assessment – Advanced

The player's risk profile is a document describing the various items taken into consideration, when enough information is gathered regarding a player, to determine the risk said player poses to the company from an AML/CFT & CPF perspective within the confines of the Business Risk Assessment created for the company.

The player risk assessment is created in one of the following situations:

- Player reaches required threshold 4000NAF (which is the sum of deposits and withdrawals),
- Player makes their first withdrawal,
- Suspicion has been raised internally regarding the player's activity,
- Change in Customer's PEP status,
- Increase in customer risk classification.

In either of the above-mentioned cases a player risk profile is drafted and is filled in using information gathered during the business relationship. Should additional control measures be applied, the response, information and documentation provided shall also be taken into account when calculating such player risk profile.

3.7 Customer Risk Profile

The customer risk profile contains the following fields:

a) Username as stored in the back office

When creating an account with the company the player selects a username that will be stored within the company back office and is used to further identify the customer. The username itself cannot be utilized to identify the customer unless access is provided to the secured company back office and thus anonymization is achieved to satisfy GDPR regulation. The only way to establish a link between the player risk profile and the player sensitive data is to have access to both platforms. Access to said platforms is carefully monitored by the company IT security team.

b) Funding method as described in the back office

The company back office stores all possible funding methods for all jurisdictions within its back office and allocates these funding methods to players using them accordingly. Each individual payment method has received an internal relevant risk score based on the strength of the controls applied on the customers using said particular payment methods, as well as on the strength of the AML policies and procedures employed by the payment method providers themselves.

f) Player deposit amount

The company considers that each deposit made by a player is crucial in determining the type of behaviour the company needs to exhibit towards the player from both an Anti-Money Laundering (AML) perspective and a Responsible Gambling perspective. The player's risk rating can increase or decrease depending on the amount of each subsequent deposit.

g) Player withdrawal amount

The company monitors each withdrawal transaction to determine the nature of the business relationship the customer intends to have with the company, as well as to set monitoring flags on the customer's account for future withdrawal actions and to identify any suspicious patterns.

c) Player Jurisdiction



The company takes into consideration player jurisdiction upon onboarding to ensure that the country the player comes from is within the company risk appetite.

All countries accepted by the platform have been analysed based on the individual controls applied by the company on a case-to-case basis, as well as concatenating information from various online resources that offer insight on the risk specific jurisdictions pose from and AML/CFT perspective. Each country supported by the platform has been given a risk score based on the data processed from the various resources.

The main documentation used for determining a country's risk rating is the following and can be found here: <https://www.baselgovernance.org/basel-aml-index/public-ranking> <https://www.knowyourcountry.com/>

d) Types of games and assessment of the behavioural model of activity

The company takes into consideration the main games played by each respective player as to understand how the player's capacity to influence the game odds and knowledge of the game mechanics can influence the capacity to circulate funds through the platform.

All games offered by the company have been broken down into the recommended categories based on the current offer.

The top 3 games played (by number of bets initiated) will be chosen and the average will count towards to final risk score. If less than 3 games have been played in total the average will change to account for the lower number of games.

e) Player registration channel (Delivery channels)

The company currently offers one type of registration, as being on the lower side of the risk spectrum (NON-FACE TO FACE DIRECTLY), especially considering that non-face-to-face relationships are no longer considered to be high risk by default.

Registration through information collection on company website – The company offers a registration form on its websites allowing players to create their own accounts and manually input their personal information. This method is rated as Medium as customers have the option of inputting erroneous information. To mitigate this, players will need to go through Due Diligence as soon as they hit any triggers mentioned in section 5 and 5.2.



4. Customer Acceptance Policy

The Customer Acceptance Policy (hereinafter the “CAP”), follows the principles and guidelines described in this document, defines the criteria for accepting new customers and defines the customer categorization criteria which shall be followed by the company and especially by the employees who have direct involvement in the obtainment of information and data relating to the customer as well as employees who will be tasked with evaluating such customer information in order to make recommendations as to whether such client falls within the Company’s risk appetite in so far as the products or services being provided are concerned.

The Compliance Officer shall be responsible for applying all the provisions of the CAP. In this respect, the Compliance Officer shall also be assisting the MLRO with the implementation of the CAP, as applicable.

The MLRO shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually, in accordance with the provisions of this policy, or at any other such interval as may be determined from time to time based on any changes in the company’s inherent and residual risk.

4.1 Failure or refusal to submit information

Customers who fail or refuse to submit and provide the company with the requisite data, information and/or documentation for their identification and verification and the creation of their profile, after they have reached the relevant thresholds (Amount of deposits and withdrawals 4000NAF, first withdrawal or due to an increase in the client risk profile after 30 days) without adequate justification, constitutes elements that may lead to the creation of a suspicion that the customer is involved in money laundering or terrorist financing activities, although this cannot be taken as an absolute and more investigation may be required before coming to such conclusion. In such an event, the company shall suspend the customer’s account or the execution of the transaction while at the same time the MLRO must also considers whether it is justified under the circumstances at hand to submit a report to the FIU.

If, during the Business Relationship or pending the execution of a transaction, the Client fails or refuses to submit, within a reasonable timeframe (30 days from the date upon which the relevant threshold or circumstances have become effective), the required verification data and information in accordance with this document, the company may inform the Client of their intention to terminate the Business Relationship, provided that in so doing it will not be tipping off the client. If signs of ML are present as a result of the investigate, the report will be sent to the FIU (UTR).

4.2 General Principles of the CAP

The General Principles of the CAP are the following:

the company shall classify customers and/or products into various risk categories and, on the basis of the risk perception attached to such classifications will determine the amount and quality of information and documentation which will be required in order for a client to be accepted or rejected.

Customers may only sign up and be allowed to make use of the company’s products and services if they provide the following information:

- a. name and surname;
- b. permanent residential address;
- c. date of birth;
- d. place of birth;
- e. nationality;
- f. identity reference number where applicable.

However, in low-risk scenarios/sign up the company may limit identification to the three personal details set out in (a) to (c) above.

All documents and data described in this policy must be collected before allowing a customer to continue making use of the services provided once the thresholds have been reached.

No services shall be provided to anonymous customers or customers who are known to be operating under fictitious names.

No services shall be provided to Extreme-risk customers unless the prospective customer is approved by senior management or the MLRO.

4.3 The Criteria in the Customer Risk Level Breakdown

This section describes the criteria for accepting new Clients based on their risk categorisation. Following a risk-based approach one must on a case-by-case basis determine what level of due diligence should be applied on identification, business relationship and transaction level, provided that these do not fall below the minimum as set out by the various applicable laws and regulations in place at the time. Whether the level of risk is above or below the threshold the Company is willing to undertake, one needs to be able to provide evidence to regulatory bodies that the appropriate steps have been taken to mitigate risk.

There are three commonly recognised categories of due diligence:

- Simplified due diligence (SDD)
- Customer due diligence (CDD)
- Enhanced due diligence (EDD)

The customer risk assessment is automated through a creation of an in-house system. This system is automated based on the five risk pillars whilst taking account of other various factors such as amount of average bet size, declared net worth, type of game, adverse media, duration of business relationship, deposit/withdrawal method and thresholds.

4.3.1 Low Risk Clients

The Company shall accept Clients who are categorised as low risk Clients as long as the general principles as defined in this policy are followed.

Low Risk (score 0-163)

Customers with a low-risk rating will need to undergo basic customer due diligence (as described in the Customer Due Diligence Procedure) when engaging in financial transactions is equal to or in excess the threshold of 4000NAF or on the first withdrawal. The customers classified as low risk will be monitored at a lower rate. Based on changes in the customer's account they can be moved to a higher risk class. Level 1 account controls will be implemented. Specific Enhanced due diligence will be requested if the case arises.

4.3.2 Medium Risk Clients

The Company shall accept Clients who are categorised as medium risk Clients as long as the general principles as defined in this policy are followed.

Medium Risk (Score 164 –334)

Customers with a medium risk score will need to undergo basic customer due diligence (as described in the Customer Due Diligence Procedure) when engaging in financial transactions is equal to or in excess the threshold of 4000NAF or on the first withdrawal. The customers classified as medium risk will be more stringently monitored (as opposed to medium-low risk customers), Level 2 account controls will be implemented. Specific Enhanced due diligence will be requested if the case arises.

4.3.3 High Risk Clients

The Company shall accept Clients who are categorised as high-risk Clients as long as the general principles as defined in this policy are followed.

High Risk (Score 335 - 500)

Customers with a high-risk score will need to undergo enhanced due diligence (as described in the Customer Due Diligence Procedure) when engaging in financial transactions is equal to or in excess the threshold of 4000NAF or on the first withdrawal. The customers classified as high risk will have the highest level of stringency applied to their ongoing monitoring. Level 3 account controls will be implemented. Full enhanced due diligence will be requested.

4.3.4 Extreme Risk

Extreme level clients will be required to undergo enhanced due diligence (as described in the Client Due Diligence Procedure) on any event requiring risk assessment. Clients classified as having an extreme risk level will be immediately restricted from financial transactions and Level 4 account controls will be implemented. Full enhanced due diligence will be requested.

4.3.5 PEPs

PEPs (Politically Exposed Persons) are not accepted by Winlink B.V.. If client change their status to PEP, they will be blocked immediately, and the funds will be remitted back to the client. The Business relationship is terminated.

5. Customer Due Diligence

Customer due diligence (CDD) involves the Company verifying customer identities, evaluating their risk profiles, conducting ongoing transaction monitoring, and performing combined sanction and PEP screening as part of a unified risk assessment process. This ensures effective prevention of money laundering, terrorist financing, and other financial crimes, while maintaining compliance with applicable legal requirements.

5.1 Simplified due diligence

This is the first stage of the process, which is carried out for the purposes of identifying and verifying the player. Registered details will be cross-checked against any documentation and public information which includes confirmation of the name, surname, date of birth and permanent residential address of the player.

New users must duly identify themselves by completing the KYC (Know Your Customer) screening upon registration providing at least the elements set out in (a) to (c) below:

- a. full name;
- b. date of birth;
- c. permanent residential address;
- d. place of birth;
- e. nationality; and
- f. identity number.

The extent of personal details verified can vary, whereby in low risk situations, the company shall verify the basic identification details, while the verification of any other personal details is risk-based, as long as the company has sufficient comfort that it knows who its customer is. In this stage verification of source of wealth and source of funds will not require an in-depth analysis of the origin of the customer's funds and the activities which have led to the accumulation of the customer's wealth as the risk of ML/TF is relatively low.

Before doing business or performing an occasional transaction for the first time with a player, the company shall check published lists of known or suspected terrorists or other sanctioned persons or companies:

a. U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List

The Company checks amendments of Sanctions Decrees and Regulations that are published on the GCB website <https://www.gamingcontrolcuracao.org/> on a regular basis and updates its Policies and procedures accordingly to reflect such amendments.

Further, at this stage all customers will be screened against PEP lists through public sources and where relevant and deemed necessary, through closed sources, with the use of a third-party provider.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

5.2 Customer due diligence

The CDD measures include:

- Identifying the player and verifying their identity using reliable, independent documents, data, or information.
- Identifying the beneficial owner and taking reasonable steps to verify their identity, ensuring the casino knows who the beneficial owner is. For legal entities and arrangements, this includes understanding the customer's ownership and control structure.
- Understanding and, when appropriate, obtaining information on the purpose and intended nature of the business relationship.
- Conducting ongoing due diligence on the business relationship and scrutinizing transactions throughout the relationship to ensure they align with the casino's knowledge of the player, their business, and risk profile, including, when necessary, the source of funds.

Identification involves collecting personal details of the player to establish their identity. Verification, on the other hand, confirms these details using reliable, independent documents, data, or information. The required personal information and the extent of verification will vary based on risk.

The company shall undertake CDD measures when:

- When players engage in financial transactions equal to or above Naf. 4,000;
- carrying out occasional transactions above the monetary equivalent of Naf. 4,000;
- there is a suspicion of money laundering or terrorist financing; or
- the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

For customer relationships that were not previously subject to full CDD, the Company applies such measures at appropriate times, on a risk-sensitive basis, in line with current standards and operational procedures.

In cases where the player's behaviour is unusual, or the value of the transaction exceeds the established average, the source of funds and source of wealth may be requested. The client will be allowed to deposit funds and use the company's products but will not be allowed to make any withdrawals until the documentation is received.

In cases where the threshold of Naf. 4,000 is reached, restrictions will apply depending on the nature of the transaction. If the threshold is reached as a result of a deposit, the player may continue to play using existing funds but will not be permitted to make further deposits or request withdrawals until verification is completed. If the threshold is reached due to a withdrawal request, the account will be fully restricted, including gameplay, until the necessary documents are reviewed and accepted. If the required documentation is not received within 30 days of its request, the company will notify the player of the intention to terminate the business relationship with the client. In case of signs of money laundering, a report on an unusual transaction will be sent to the FIU.



5.3 Enhanced due diligence

Enhanced due diligence (EDD) checks of the customer may be initiated resulting from hits on PEP-lists, residency in high-risk geographical areas and through various financial or behavioral triggers. The customer/enhanced due diligence should also be followed in the following circumstances:

- a. Upon any single or cumulative transaction, be it a deposit amounting to USD 10,000, the player will be obliged to send a proof of proof of funds as part of the enhanced due diligence. This will be done by requesting by the player to declare his/her net worth or annual income and explain the activities leading to the accumulation of wealth. Afterwards, the player will proceed to submit proof of source of wealth according to what he declares.
- b. When there is a material change in the risk and is classified as a high-risk client.
- c. When there is a suspicion about the customer profile in terms of source of wealth and the customer profile in general.

Depending on the nature of the reason that triggered the EDD, the following measures may be undertaken by the Company:

- a. Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- b. Obtaining additional information on the intended nature of the business relationship;
- c. Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- d. Obtaining information on the reasons for intended or performed transactions;
- e. Obtaining the approval of senior management to commence or continue the business relationship;
- f. Conducting enhanced monitoring of the business relationship;
- g. Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

No further transactions may be processed until these documents are sent by the customer and are checked and verified by the management.

Upon registration of a new customer, their transactions and betting behaviour will be checked and monitored daily. Mechanisms are in place that enforce a one account per person policy, and if an issue of multiple accounts is detected all relative accounts are suspended/frozen until the matter is resolved. Scripts are in place that detect strange or unusual behaviours from our clients. This procedure enables the company to analyse the way every individual uses the products from our website, making it possible to categorize the players and thus set limits to the individual players according to their betting habits.

5.4 Registration Procedure

In order to be able to participate and play on Winlink B.V. websites players need first to be registered and create a player account, following the Winlink B.V. Registration Process. Winlink B.V. system does not allow Customers who do not register on the website to place any stakes on any of the offered games and perform automatization checks on the information provided by Customers in order to ensure that this information has not been re-used in the past to register another Player due to one account per player condition.

During the registration process, Winlink B.V. does not accept clients under 18 years of age or clients from countries with restricted rights. In order to open an account and access services at Winlink B.V., including demo games which are available through the same account used for paid games, the customer must submit a registration application and provide the following mandatory information:

- First Name and Last Name,



- Full permanent residential address
- Date of Birth
- Correct e-mail address. (include respond for verification link)
- Mobile number (include verification call or SMS)
- Username
- Password

If Winlink B.V.'s System or employees detect that the information provided is not valid, complete, correct or up-to-date or the Customer tried or managed to register an account with false information (particularly: first and last name, mobile number, e-mail address, username), Winlink B.V.'s employees shall review the case and either request for new information with the temporary suspension of these accounts until they are satisfied that the process and the new information provided is correct, or permanently close these Accounts and report the case to the MLRO.

Winlink B.V. must prevent scenarios wherein a customer tries to open duplicate accounts by carrying out a daily check from the list of new registrations. If the information provided matches an existing account and if any of them were used to register in another account, then Winlink B.V.'s employees temporarily close the accounts and request for KYC(id documentation).

If a customer declares a different country of registration from his actual country of residence -> daily check from the list of new registrations if the IP address of each customer corresponds to the country declared as country of residence in the registration form. If the IP address does not match the Country of Registration, Winlink B.V. shall ask the client for a clarification. Afterwards, the employees shall monitor the location according to time frames provided by client and proceed accordingly. If there is a reasonable suspicion about the mismatch of the IP with the timeframes, the employees should proceed with temporarily close the account and request for KYC. (utility bill)

Each new customer has to provide a copy of an ID document (passport, ID card or driving license) when relevant thresholds are reached. In cases where a permanent address is not indicated on the ID document, the user will be asked to provide a copy of a utility bill and/or a bank statement showing name and address, but not a mobile phone bill.

Furthermore, the identity check may include additional measures such as the provision of a copy of each credit card used in the specific account.

Any remaining doubts concerning the identity of a customer have to be reported based on the Procedure detailing reporting lines. In such a case, further investigations have to be started.

These may include:

- Check of the IP used by the customer.
- Check of the provided phone number and/or call to the provided phone number.
- Internet research on the customer details.
- Request to the official authorities in the country of the customer – this has to be done by compliance management.

The due diligence documentation criteria are set as follows:

- I.D documents must be official documents issued by a government entity that includes confirmation of the name and residential address or date of birth and a photo such as a passport can be used to verify an identity. Where this type of documentation is not available a government issued document confirming the name of the individual and supporting document supplied by a public authority, court or a financially regulated service provider that includes the individuals full name and either date of birth or residential address can be used.
- The details in the passport are compared to other documents collected at the company's discretion.
- When in doubt of forgery, the player is requested to hold up the passport to his/her face in order to verify that such passport belongs to the said individual.
- Online public databases are checked in order to cross check the information in the documents provided.
- Public searches through social media and other sources are checked in order to build the player profile.

If the customer comes from a high-risk jurisdiction, the enhanced due diligence process is kicked in immediately and the account is monitored closely. It is at the operator's discretion to refuse registrations from high-risk jurisdictions.

5.5 Sanction list Screening:

The company shall on the occurrence of the following events or when it deems it fit and proper to do so, conduct a screening of the relevant sanction using published sanctions lists and an internally implemented screening mechanism. Upon registration, client will be screened against relevant sanctions lists issued by the United Nations, the Office of Foreign Assets Control (OFAC) or the European Union or any other relevant body responsible for imposing sanctions.

Such screening will then be conducted periodically based on the client risk assessment conducted but in any case at the time of registration, at the time CDD is conducted, at the moment of a withdrawal request, when any material changes to the client's profile occur. The frequency of such sanction list screening will be increased should a player reach the 4000NAF threshold. Moreover, if there is an investigation behind a possible hit, the client's risk score should be deemed as high, and more monitoring is applied until the investigation concludes itself.

In the event that company becomes aware that one of its clients, or potential clients is subject to an international Sanction, or has ties to countries or entities subject to such sanctions, the company must immediately inform without delay the MLRO, who in turn must report this to the FIU.

All appropriate measure must be taken to ensure that any assets including funds held on behalf of such individual are frozen immediately until further instructions are given by the FIU.

5.6 Player Verification Procedure

Players will be requested to provide mandatory due diligence documents during the following stages:

- Once the Player reaches the 4000NAF threshold
- Upon request for the first withdrawal
- At any other stage that Winlink B.V.'s system or employees detect any suspicious behaviour of the Player or have any doubt on the accuracy of the information provided during the Registration Process or a Player Account classified as High Risk.

Players are obliged to provide Winlink B.V. with documents which verify their identity and Address. Winlink B.V.'s employees should oversee this procedure and, where any red flags are raised or registration has been rejected and are unable to complete the process, the employees should review the provided documents and the reasons for rejection. In such cases, Winlink B.V. employees should thoroughly check all the documents provided and any third-party verification reports, and reconsider whether the documents should be accepted or rejected, and in case of rejection, whether to request the customer to provide new documents or suspend the account and report the case to the Head of Compliance/MLRO in line with the company's internal reporting procedures.

Winlink B.V. employees, in terms of Player verification Process, shall review the following documents:

a) Documents needed to verify Players' identity (including a clear, colour, scan or photo alongside with a selfie picture) of any of the following:

- Official ID card
- Passport
- Driving License

Note: If the casino obtains foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly when the type of document is unfamiliar.

b) Documents needed to verify Players' address:

Players should follow Winlink B.V. website instructions and provide a clear scan, colour photo, PDF or screenshot of



any official document addressed to them, issued within the last 6 months, stating their full name and current address.

This can include one of the following:

- Utility bill (electricity, water, gas, landline phone bill, internet line account)
Bank statement or reference letter
- A rental or lease agreement
- Any correspondence from a central or local government authority, department or agency or any other government-issued document.

c) Any additional documents:

At any stage, Players may be asked to provide any further information to those already provided or any additional documentation at Winlink B.V.'s team sole discretion.

Upon receiving the required documents and in order for the player's account to be validated, Winlink B.V.'s team shall conduct a manual check on the information/documentation received and consider whether more information/documentation is needed.

The following checks are to be performed:

- Check whether the player's personal data listed in the provided documents match the provided information during the registration.
- Cross-Check of any third-party report on similarity check and whether the selfie meets the system requirements (clear photo of player's entire face without wearing glasses, hats, scarves, or any other accessory that covers the face, in whole or in part) have been adhered to.
- Make sure that system does not allow registration of Players who are underage, coming from restricted countries or have another player Account in their name.
- Manual Check of documents provided to verify Players' address
- Verify the validity and authenticity of the provided documents, verify and confirm that the documents contain all necessary information, according to the information it is meant to verify

5.7 Minor Prevention Procedures

Winlink B.V. follows strict rules about underage gambling and does not allow players under the age of 18 to be registered or maintain an account. Winlink B.V. also aims to better protect underage players and strictly follows specific procedures in exceptional cases in which an underage manages to register and use a Winlink B.V. Player Account.

To access the services, the Customers are required to enter information about their date of birth. Based on this information, the system makes the calculations (taking into consideration the given date of birth and the current date of registration) and does not allow players under the age of 18 to be registered.

In exceptional cases in which an underage manages to register and uses a player account by giving false information when registering, Winlink B.V.'s team shall proceed to the following corrective measures:

- Suspend the account and freeze any available amounts until the whole process is concluded.
- Request for full KYC for both underage and one of his/her parents.
- Refund to the parent's or any other third-party verified Bank Account of the entire amount deposited by the underage and keep any winnings or bonuses given by Winlink B.V. Limited.
- Permanently closure of this account.



5.8 Politically Exposed Persons:

Winlink B.V. will not accept PEP, however this section relates to a possible scenario wherein PEP start being accepted. Therefore, in such circumstance the below is noted.

Winlink B.V. is aware of its duties towards identifying and carrying out due diligence in terms of politically exposed persons. The company shall apply the following with respect to the accounts of “Politically Exposed Persons”:

a) The establishment of a Business Relationship or the execution of an Occasional Transaction with persons holding important public positions and with natural persons closely related to them, may expose the Company to enhanced risks, especially if the potential Client seeking to establish a Business Relationship or the execution of an Occasional Transaction is a PEP, a member of his immediate family or a close associate of or is known to be associated with a PEP.

The Company shall pay more attention when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering laws and regulations are not equivalent with international standards or who have been flagged as having regulatory deficiencies by the FATF or any other regulatory and/or monitoring authority.

b) In order to effectively manage such risks, Winlink B.V. shall assess the countries of origin of its Clients in order to identify the ones that are more vulnerable to corruption or maintain laws and regulations that do not meet the 40+9 requirements of the FATF.

5.8.1 The meaning of a ‘Politically Exposed Persons’:

A PEP is a natural person who is or has been entrusted with a prominent public function, other than middle ranking or more junior officials. Public functions which are considered as prominent public functions and would therefore render the holder thereof a PEP include but are not limited to:

- Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries;
- Members of Parliament or similar legislative bodies;
- Members of the governing bodies of political parties;
- Members of the superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- Members of courts of auditors, or of the boards of central banks;
- Ambassadors, charge d’affaires and other high-ranking officers in the armed forces;
- Members of the administrative, management or supervisory boards of state-owned enterprises;
- Permanent secretaries within all the Government ministries;
- Chiefs of staff within all the Government Ministries;
- The Commissioner and Deputy Commissioners of Police;
- Anyone exercising a function equivalent to those set out above within any international body. EDD measures on a risk-sensitive basis must be applied.

5.8.2 Measures Applied to PEPs

Without prejudice to the application, on a risk-sensitive basis, of enhanced Client due diligence measures, where a person has ceased to be entrusted with a prominent public function within the meaning of this section 5.5 or a **period of at least one year**, Winlink B.V. shall not be obliged to consider such a person as politically exposed. Nevertheless, the Company may still consider a person to be politically exposed notwithstanding that he no longer holds an office or role which had rendered him to be considered as a PEP for a period longer than 12 months. Such decision will be based on the risk associated with the position the person had held when being considered as a PEP.



Persons known to be close associates' includes the following:

- any natural person who is known to have joint Beneficial Ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in section 5.5 above
- any natural person who has sole Beneficial Ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to in section 5.5 above.

f) Without prejudice to the provisions of this document, Winlink B.V. will adopt the following additional due diligence measures when it establishes a Business Relationship or will carry out an Occasional Transaction with a PEP:

Winlink B.V. puts in place appropriate screening procedures to enable it to determine whether a prospective Client is a PEP. Such procedures may include, depending on the degree of risk, the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the Client himself or from publicly available information.

The decision for establishing a Business Relationship or the execution of an Occasional Transaction with a PEP is taken senior management approval for establishing or continuing business relationships with such persons.

Before establishing a Business Relationship or executing an Occasional Transaction with a PEP, the company shall obtain adequate documentation to ascertain not only the identity of the said person but also to establish the source of wealth and source of funds that are involved in business relationships or transactions with such persons.

The Company shall conduct enhanced, ongoing monitoring to PEP Gaming Activity and transactions (pay-in and pay-out).

The player will be categorized as a Extreme-Risk Player.

The profile shall be regularly reviewed and updated with new data and information.

The account shall be subject to a shorter review period than would otherwise be assigned for a client of a similar risk, in order to determine whether to allow its continuance of operation.

Winlink B.V. is required to obtain a higher standard in relation to the quality of documents obtained- certified documents are one example.

If a Winlink B.V. identified the user to be included in any Sanction List or wanted for offenses relating to money laundering, his Player Account shall immediately be closed and reported to the Head of Compliance.

Winlink B.V. may carry out or, in the case of applying enhanced on-going monitoring, implement these measures at any point in time between the establishment of the business relationship and the point in time when the 4000NAF threshold is met, but not later from the lapse of thirty days from when the said threshold is reached.

Should a customer who had not been identified as a PEP at on-boarding stage result to have become one, the Company will carry out or implement obtain senior management approval to terminate the business relationship with the PEP immediately.

6. Record Keeping and Monitoring

6.1 General

The Administration Department of the Company shall maintain records of:

- a) the Client identification documents obtained during the Client identification and due diligence procedures, as applicable; and
- b) the details of all relevant records with respect to the provision of investment services to Clients.

The documents/data mentioned above shall be kept for a period of at least five (5) years, which is to start running either from the termination of a business relationship or from the date on which an occasional transaction has been executed. It is provided that the documents/data mentioned in points (a) and (b) above which may be relevant to ongoing investigations shall be kept by Winlink B.V. until the FIU confirms that the investigation has been completed and the case has been closed. Furthermore, should the company require the documents for the institution, prosecution or to defend against any claim for which a longer prescriptive period exists, than such records will be kept until such time as the claim is extinguished or such prescriptive period has elapsed.

6.2 Format of Records

The Administration Department shall retain the documents/data mentioned in this Policy, other than the original documents or their Certified true copies that are kept in a hard copy form, in other forms, such as electronic form, provided that the Administration Department shall be able to retrieve the relevant documents/data without undue delay and present them at any time, to the FIU or any other relevant authority, after a relevant request.

In case the company will establish a documents/data retention policy, the MLRO shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive. The Internal Auditor shall review the adherence of the company to the above, at least annually.

7.0 On-going Monitoring Process

7.1 General Provisions of On-going Monitoring Process

The regular monitoring of the Clients' accounts and transactions is an imperative element in the effective controlling of the risk of Money Laundering and Terrorist Financing. In this respect, the MLRO shall be responsible for maintaining, as well as developing the on-going monitoring process of the Company.

7.2 Procedures of On-going Monitoring Procedures

The procedures and frequency relating to the monitoring of customers' profiles, accounts, and examination of transactions based on the client's level of risk shall include the following:

- Identification of:
 - Transactions that, by their nature, may be associated with money laundering or terrorist financing.
 - Unusual or suspicious transactions that are inconsistent with the client's economic profile, for the purposes of further investigation.
- In the case of any unusual or suspicious transactions, the administrator handling the specific client, as well as the head of the relevant department, shall be responsible for communicating with the MLRO.
- Investigation of unusual or suspicious transactions by the MLRO, with the results recorded separately and kept in the file of the clients concerned.

- Ascertainment of the source and/or origin of the funds credited to accounts.
- Use of appropriate IT systems.

To comply with its monitoring requirements, the Company shall review the client's file according to the timeframes outlined in section 7.3 below, taking into consideration the following to assess whether any additional or replacement documentation/evidence might be required:

- Tracking expiry dates of identification documents and refreshing them in a timely manner before or as they approach expiration.
- Update of any changes in the client profile.
- Changes in the client's activities that might impact the client's economic profile.
- Reviewing ways in which new products and services may be used by criminals for money laundering and/or terrorist financing, and how these methods may evolve to conceal such illicit activities.
- The compliance officer performs checks to ensure that the relevant reviews take place and that documentation is kept accordingly.
- Reporting and accountability by the compliance officer to the Board of Directors and Senior Management.
- Liaising with the Gaming Control Board (GCB), FIU, or any other relevant authority when required.

7.3 Timeframes

The time frames set below shall act as guidelines for the compliance officer when setting the dates for the re-review dates. Such time frames may be changed if justified notwithstanding the client has been risked as in a category, provided such justification is recorded. Furthermore, these time frames shall be changed and updated should any of the factors effecting the risk the client poses will change. The below time frames shall be taken as guidance points and not as a mandatory rule.

Risk Classification Time Frames:

Low Risk: 36 months to 60 months

Medium Risk: 18 months to 36 months

High Risk: 12 months to 18 months

7.4 Pay-out Management Procedure

Checks to be performed on each pay-out:

a) Account check

The owner of the gaming account must be the same person as the owner of the bank account or credit card. All account information, like address, email, date of birth etc., must be complete and authentic. Withdrawals will be made to the same source where the funds originated (where possible).

b) Deposits must have been used

On each pay-out, the company will verify whether the deposits have been used for stakes. All deposits need to have been wagered at least three (3) times when a bonus was not credited before a withdrawal request can be made.

A pay-out cannot be processed if the deposited amount has not been used for stakes. If the deposited amount has not been used, the pay-out should be denied. Furthermore, the latest winnings should be checked for correctness.

c) Fulfilment of bonus rules

Fulfilment of bonus rules before a pay-out can be deducted from the client's account, the account has to be checked if a bonus has been given to the client since the last pay-out. When a bonus has been credited, the account has to be



checked for fulfilment of the bonus rules applicable to that bonus. If bonus rules have not been fulfilled the requested pay-out cannot be completed.

d) Deposit funds

Funds deposited in the gaming wallet can only be used for gaming activity. Should Winlink B.V. notice regular changes by players to the payment method linked to the gaming wallet, the account will be temporarily suspended until the necessary explanations are provided by the player for these changes.

Winlink B.V. does not allow players to transfer funds between accounts under any circumstances. Winlink B.V.'s KYC team continuously monitors players' deposit activity as well as has automated processes in place to receive notifications when players reach the 4000NAF threshold.

7.4.1 Risk Profile for Winlink B.V.

The risk profile and Risk appetite for Winlink B.V. will be calculated based on the Business Risk Assessment done at a minimum once every year. The Business Risk Assessment will take into consideration all Risks the company faces constantly as well as the mitigating factors controlling the inherent risk.

Modifications will be done to the policies and procedures for Winlink B.V. on the basis of the resulting residual risk, as soon as the need arises. Withdrawals can only be paid to the same client's account used to deposit money. In the event that the payment method used does not allow for Winlink B.V. to settle payouts to the same payment method, then Winlink B.V. must identify and verify that the method used to settle the withdrawal request belongs to the player in question.

Winlink B.V. does not accept cash from customers, and funds may only be received through online transfer. In the same manner no withdrawals can be processed as cash. Withdrawals will always be remitted to the same account from where the funds originated, or to an account or payment method which has been verified as belonging to the player.

DD documentation is always requested and verified for all players effecting a single or cumulative transaction of 4000NAF or upon requesting to withdraw funds.

The system will automatically stop minors from playing as players inputting a date of birth below the age of 18 years of age or the applicable age within their country of residence will not be able to complete the registration process.

7.5 Accounts accessed through VPN

The below procedure is to be followed in scenarios where the company becomes aware by whatever means, that a player has made use a VPN to access and make use of the accounts held with the company. This applies to instance where the use of VPN is to hide, obscure, or otherwise conceal the true geographic location of the player.

Should it transpire that a player is making use of a VPN for the above mentioned or similar reasons, the company will restrict the player's account by applying any or all of the measures below including but not limited to:

- Suspending and/or blocking of withdrawal requests, until such time as the player has completed verification process or in the instance that such process has already been completed, until such time as the player's true geographic location can be ascertained;
- suspending the player's account;
- impose deposit limits and/or suspending the player's ability to deposit further funds into the accounts held with the company;
- File an internal unusual activity report indicating any and all reasons why the player's activity is deemed suspicious. Such report should include any and all available information and supporting documentation in relation to the player and his activities;
- Initiate due diligence procedures in the event that such procedure has not been initiated and/or completed yet;
- Obtain confirmation and verification of the player's actual geographic location if this has not been detected by the company's internal systems;



Once the player's actual geographic location is determined, the company has to then confirm and ensure that it is duly authorised to provide such products/services on the basis of the licenses it holds at the time of the detection. In the event that it is determined that such service cannot be legally provided, the company must stop all of the player's activity and take the necessary steps to close-off the account.

In all of the above instances when the company makes a request to a player for any clarification, information or supporting documentation, the player shall have 30 days to abide by such requests. Failure to do so, should result in the immediate suspension and eventual termination of the player's account. In case if ML suspicions the MLRO should be notified immediately and by not later than 24 hours from when such term has expired.

The company should also update the player's CRA accordingly and increase the risk rating if it is deemed appropriate to do so.

It is advisable for the company to obtain legal opinions with regards to jurisdictions which are detected through the VPN, which jurisdictions are not covered by the company's licenses at the time of detection. Such legal opinions should indicate whether the company is authorised to provide its products/services in that particular jurisdictions. The company should abide with the recommendations made in such legal opinions so as to ensure that it is not in breach of the laws of the detected jurisdiction.

8. Unusual Activity/Transaction Reporting

In any subjective cases where the company encounters, verifies or there exists a reasonable suspicion that any form of money laundering is taking place or being attempted, such activity will be reported to the Financial Intelligence Unit (FIU), as required.

In cases with an objective indicator, if a player is found in transactions equal to or exceeding the threshold of 5000NAF, a report will be sent to the FIU. The threshold of 5,000 NAF is monitored on a per gaming day basis, taking into account the cumulative value of relevant transactions. This applies to relevant transaction types as defined under the applicable indicator framework, regardless of the payment method used.

The activity will be reported through the portal for filing and submitting of unusual transaction reports (UTR) and Unusual Activity reports (UAR), as designated by the FIU.(currently goAML portal). The company through its MLRO is responsible to ensure that when an UTR/UAR is filed, all supporting documentation and information pertaining to why the transactions, as well as the player has been flagged as suspicious must also be submitted. Any employee and/or company officer having suspicion that a client is involved in any stage of ML or TF&CPF, is attempting to launder money using the products and/or services of the company must report such suspicion to the MLRO by not later than 24hours from when such suspicion is formed. The MLRO, upon receipt of such report, must initiate an investigation into the unusual activity and/or transaction and verify if such suspicion is objectively justified. This is to be done in the 10 working days. This notwithstanding, the MLRO may still continue to investigate to gather the evidence required to submit a complete UTR/UAR.

The definition of a unusual transaction as well as the types of unusual transactions which may be used for Money Laundering and Terrorist Financing are almost unlimited. Suspicion of ML/TF&CPF is subjective, and one must consider a number of circumstances together in order to be able to come to a reasonable conclusion that suspicion does indeed subsist. A unusual transaction or activity will often be one which is inconsistent with a client's known, transaction pattern/activities or with the normal deposit/wagering activity of the specific client, or in general with the economic profile that the company has created for the client. The company shall ensure that it maintains adequate information and knows enough about its client's activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.



8.1 Knowledge

Knowledge may be deemed to be an objective criterion and therefore it is not difficult to ascertain whether there is ML/FT. If for any reason the MLRO, or any other employee of the company, is aware or is in possession of information that indicates that any of the above activities may have taken place, are taking place, or will be taking place, the MLRO should immediately inform through an internal report and then a decision is taken on whether filing a report with the FIU is necessary or not depending on the strength of likelihood that with the information in hand there is reasonable suspicion to report the player.

8.2 Unusual Transactions

The definition of a unusual transaction as well as the types of unusual transactions which may be used for Money Laundering and Terrorist Financing are vast. Suspicion of ML/FT is subjective, and one must consider a number of circumstances together in order to be able to come to a reasonable conclusion that suspicion does indeed subsist. A unusual transaction will often be one which is inconsistent with a client's known, legitimate business or personal activities or with the normal business of the specific client, or in general with the economic profile that the company has created for the Client. The company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

Examples of what might constitute unusual transactions/activities related to Money Laundering and Terrorist Financing are listed after this paragraph. The relevant list is neither exhaustive nor it includes all types of transactions or services that may be requested to be used, nevertheless it can assist the company and the team in recognising the main methods used for Money Laundering and Terrorist Financing in relation to Remote Gaming.

The detection by the company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds for the payments and intended transactions, the nature and economic/business purpose of the underlying transactions requested, and the circumstances surrounding the particular activities.

a) The following is a list of possible red flags which company may wish to consider:

- Customer deposits or withdraws amounts equal to or exceeding 5000NAF.
- Customer deposits or withdraws amounts close to but below the threshold, clearly trying to avoid additional checks.
- Customer does not cooperate in the carrying out of CDD.
- Customer attempts to register more than one account with the same licensee.
- Customer deposits considerable amounts during a single session by means of multiple pre-paid cards.
- Customer deposit funds well in excess of what is required to sustain usual betting patterns.
- Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the customer's wealth, income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Customer displays suspicious behaviour in playing games that are considered as high risk.

b) In order to identify unusual transactions, the MLRO shall perform the following activities:



- Monitor on a continuous basis any changes in the client's financial status, business activities, type of transactions etc
- Monitor on a continuous basis if any client is engaged in any of the practices described in the list containing examples of what might constitute unusual transactions/activities related to Money Laundering and Terrorist Financing which is in the abovementioned list.
- Provide any adequate training to any and all staff who will be in contact with any client, agents, client's officers, client's representatives, client's transactional information and/or documentation client's, operational information and/or documentation and any other information and/or documentation which can lead to knowledge or suspicion being detected.

c) Furthermore, the MLRO shall perform the following activities:

- Receive and investigate information from Winlink B.V.'s team, on unusual transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report or any other form which may be deemed appropriate from time to time in accordance with the urgency and severity of the situation. The said reports are archived by the MLRO;
- evaluate and check the information received from Winlink B.V.'s team, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLRO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;

If, as a result of the evaluation described above, the MLRO decides to disclose this information to the FIU, he prepares a written report and submits it accordingly. In connection with such decisions, the MLRO also assesses whether temporary restriction of access to the player's funds is warranted. This consideration is based on contextual risk factors, including the status of verification and the potential risk of tipping off the customer.

8.3 MLRO's Report to the FIU

All the reports of the MLRO relating to UAR/UTR are submitted through the goAML portal. After the submission of UTR/UAR reports, the company may subsequently wish to terminate its relationship with the client concerned for de-risking reasons or to keep the account suspended until further notice/information is obtained from the FIU. In such an event, the company exercises caution, according to the Law, not to alert the client concerned that a suspicious report has been submitted to the FIU. Close liaison with the FIU is, therefore, maintained in an effort to avoid any frustration to the investigations conducted. If no information and/or directions are given by the FIU, it shall be up to the company to decide on the best course of action, whilst at all times ensuring that no tipping-off takes place.

Furthermore, after the submission of a unusual transaction/activity report, the Clients' gaming accounts and services rendered concerned as well as any other connected accounts are placed under the close monitoring of the MLRO and cease to be operative if deemed appropriate to do so without tipping off or risking tipping off the reported individual or entity.

8.4 Submission of Information to the FIU

Winlink B.V. shall ensure that in the case of a unusual transaction investigation by the FIU, the MLRO will be able to provide without delay the following information:

- a) the identity of the holders for which the services have been provided;
- b) data of the volume of funds or level of transactions used for the services being rendered and flowing through the accounts created for the Player;
- c) connected accounts, if any;

d) in relation to specific transactions:

- the origin of the funds
- the type and amount of the currency involved in the transaction
- the form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers
- the destination of the funds
- the type and identifying number of any account involved in the transaction.
- any other information which is available and deemed to be essential to the investigation

e) In order to identify unusual transactions, the MLRO shall perform the following activities:

- Monitor on a continuous basis any changes in the client's financial status, business activities, type of transactions etc
- Provide any adequate training to any and all staff who will be in contact with any client, agents, client's representatives, client's transactional information and/or documentation client's, operational information and/or documentation and any other information and/or documentation which can lead to knowledge or suspicion being detected.

The MLRO shall belong hierarchically to the higher ranks of the Company's organisational structure so as to command the necessary authority. Furthermore, the MLRO shall lead the Company's Money Laundering Compliance procedures and processes and report to the Senior Management. The MLRO shall also have access to all relevant information necessary to perform his/her duties.

Where the report is based on the objective indicators, as outlined by pertinent Curacao legislation, such reports shall be submitted to the FIU within 48 hours of the transaction taking place.

Where the report is based on the subjective indicators, as outlined by pertinent Curacao legislation, such reports shall follow the timeline below:

- Internal UTR must be submitted to the MLRO within 24 hours of the transaction taking place;
- MLRO must determine the reportability of the transactions within 10 working days;
- If the MLRO determines that the transaction and/or behavior is indicative of ML/TF, the MLRO must submit the report to the FIU within 48 hours of making that determination.

8.5 Duties and Responsibilities of the Money Laundering Reporting Officer (MLRO)

Furthermore, the MLRO shall perform the following activities:

- Receive and investigate information from the Winlink B.V.'s team, on unusual transactions which creates the belief or suspicion of money laundering. This information is reported on the Internal Suspicion Report or any other form which may be deemed appropriate from time to time in accordance with the urgency and severity of the situation. The said reports are archived by the MLRO;
- evaluate and check the information received from the employees of the Company, with reference to other available sources of information and the exchanging of information in relation to the specific case with the reporter and, where this is deemed necessary, with the reporter's supervisors. The information which is contained on the report which is submitted to the MLRO is evaluated on the Internal Evaluation Report, which is also filed in a relevant file;
- if, as a result of the evaluation described above, the MLRO decides to disclose this information to the FIU, then he prepares a written report, which he submits to the FIU.
- to detect, record, and evaluate, at least on an annual basis, or on the happening of any event which might have an impact on the overall risk, all risks arising from existing and new Clients, new financial instruments and services and update and amend the systems and procedures applied by the company for the effective management of the aforesaid risks should it be required and appropriate to do so;
- to evaluate the systems and procedures applied by a third party with whom the Firm has entered into a reliance agreement in terms of Customer Due Diligence including Client Identification and Verification of the Customer, Identification & Verification of Beneficial Owners as well as the Purpose & Intended Nature of the Business

Relationship applied, and approves the cooperation with such third-parties;

- to ensure that all the branches and subsidiaries of the Company, if any, have taken all necessary measures for achieving full compliance with the provisions of this document, in relation to Client identification, due diligence and record keeping procedures;
- to provide advice and guidance to the employees of the Company on subjects related to money laundering and terrorist financing;
- to acquire the knowledge and skills required for the improvement of the appropriate procedures for recognising, preventing and obstructing any transactions and activities that are suspected to be associated with money laundering or terrorist financing
- to determine and whether the Company's departments and employees require further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organising appropriate training sessions/seminars. In this respect, the MLRO shall prepare and apply an annual staff-training program. Also, the MLRO assesses the adequacy of the education and training provided;
- to respond to all requests and queries from the FIU and provide all requested information and fully cooperate with the FIU, if required; to maintain a registry which includes the reports of unusual transactions, and relevant statistical information (e.g. the department that submitted the internal report, date of submission to the MLRO, date of assessment, date of reporting to the FIU), the evaluation reports and all the documents that verify the accomplishment of his duties.
- To review the Client's files and Client Questionnaire and to approve or reject prospective High-Risk Clients.
- to develop and establish the Client Acceptance Policy and submit it to the Directors for consideration and approval; to review and update this document as may be required from time to time, and for such updates to be communicated to the Directors for their approval, at least annually or at any such period as may be deemed necessary by the MLRO
- to monitor and assess the correct and effective implementation of the policy practices, measures, procedures and controls and in general the implementation of the AML Policies and Procedures. In this respect, the MLRO shall apply appropriate monitoring mechanisms (e.g. on-site visits to different departments of the Company) which will provide him with all the necessary information for assessing the level of compliance of the departments and employees of the Firm with the procedures and controls which are in force. In the event that the MLRO identifies shortcomings and/or weaknesses in the application of the required practices, measures, procedures and controls, shall give appropriate guidance for corrective measures and where deems necessary informs the Directors and Senior Management

9. Training

The company must ensure that training and updates are provided to staff and key persons involved in the prevention of AML and fraud within the company. Such training may be in-house or from third party providers. All training provided should be in line and in proportion to the roles and duties of the individual employee. Training should be tailored to the tasks of team members and duties of such, and the company should not adopt a one size fits all approach. However, a yearly refresher course should be provided to ensure that all staff are up to date on recent developments.

Records of such training received must be kept on file as proof of attendance of such training.

9.1 Employees' obligations

The Company will only contract with and hire individuals of good standing. When hiring new staff, the Company makes sure to collect an appropriate level of due diligence to verify the age and identity of a new employee and to allow for background checks. For key positions in the company, responsible for crucial areas within the business, more extensive measures for due diligence are carried out. Such checks will also take place periodically and when triggered by any event that impacts the position and responsibilities of the employee with a view of increasing their risk exposure.



The following documentation will be collected from all employees;

- Copy of ID;
- Information on employment history and references;
- A police conduct report will also be collected to ensure new staff do not have a criminal record.

The Company's employees shall be personally liable for failure to report information in relation to any knowledge or suspicion, regarding money laundering or terrorist financing.

The team members must cooperate and report internally, without delay, and by not later than 24 hours, anything that comes to their attention in relation to transactions for which there are grounds for suspicion that the person is involved in money laundering or terrorist financing

According to the applicable Law, the company's team shall fulfil their legal obligation to report their suspicions regarding Money Laundering and Terrorist Financing, after their compliance with point (b) above.

9.2 Employees' Education and Training

(a) The MLRO shall ensure that the employees are fully aware of their legal obligations according to the applicable Laws, regulations, directives, and implementing procedures by introducing a complete employees' education and training program;

(b) the timing and content of the training provided to the employees of the various departments will be determined according to the needs of Winlink B.V.. The frequency of the training can vary depending on the amendments of legal and/or regulatory requirements, employees' duties, but at least once a year.

(c) the training program aims at educating the Winlink B.V.'s team on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose;

(d) the training program will have a different structure for new and existing team members, and for different departments of the company, according to the services that they provide. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

9.3 MLRO Education and Training Program

The MLRO shall be responsible for any updates in the Law and attend any external training necessary. Based on his/her training the MLRO will then provide training to the employees. The main purpose of the MLRO training is to ensure that relevant employee(s) become aware of:

- the Law and the Directive
- the Firm's Anti-Money Laundering Policy
- the statutory obligations of the Firm to report unusual transactions
- the employees own personal obligation to refrain from activity that would result in money laundering
- the importance of the Clients' due diligence and identification measures requirements for money laundering prevention purposes.

10. Independent Audit Function

The Company shall be monitored and evaluated at least annually by an adequately resourced internal audit department or an outside independent party. The audit shall be performed by sufficiently qualified persons and shall be independent, thus performed by people not involved with the organization's AML compliance staff. The audit tests shall include at a minimum:

- An evaluation of the institution's anti- money laundering, counter terrorist financing and counter financing of proliferation manuals;



- Customer's file review;
- Compliance management;
- Performance of transaction testing;
- Assessment of training adequacy;
- Assessment of compliance with applicable laws and regulations;
- Evaluation of the system's ability to identify unusual activity;
- Interviews with employees who handle transactions and with their supervisors;
- A sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- An assessment of the adequacy of the record retention system.

The testing scope and results shall be documented. Any deficiencies are to be reported to senior management and the designated officers, with a request for prompt corrective actions to be taken by a specified deadline. The audit will also consider whether senior management was responsive to earlier audit findings.

11. Appendices

11.1 Appendix A I Suspicious Activity Report

Report prepared by:	
Company's Name	Winlink B.V.
Website	www.
Account ID	
Address	
Email address	
Telephone number	
Is identification and address verification held?	
Is enhanced due diligence held?	
Reason for suspicion	
To include: Identification verification criminal conduct known or suspected Transaction details Timestamp in UTC	
Date of report	
Receipt of report acknowledged	
Signed MLRO	
Date	

11.2. Appendix B | Prohibited countries

Afghanistan	Libya
Aland Islands	Lithuania
Albania	Mali
Algeria	Malta
American Samoa	Martinique
Angola	Mayotte
Aruba	Montenegro
Ascension and Tristan da Cunha	Myanmar (Burma)
Australia	Netherlands
Austria	New Caledonia
Barbados	Nicaragua
Belgium	Norfolk Island
Bonaire	Northern Mariana Islands
Botswana	Pakistan
British Indian Ocean Territory	Palau
Bulgaria	Palestine
Burundi	Philippines
Cambodia	Pitcairn Islands
Central African Republic	Portugal
Czech Republic)	Puerto Rico
China	Reunion
Cocos (Keeling) Islands	Romania
Colombia	Saba
Cuba	Saint Barthelemy
Curaçao	Saint Helena
Cyprus	Samoa
Democratic Republic of the Congo	Sint Eustatius
Ecuador	Somalia
Estonia	South Georgia and the South Sandwich Islands
Falkland Islands	South Sudan
Fiji	Spain
Finland	Statia
France	Sudan
French Polynesia	Sweden
French Southern and Antarctic Territories	Syria
Georgia	The Democratic People's Republic of Korea
Germany	The United States of America
Greece	Tokelau
Guadeloupe	Trinidad & Tobago
Guam	Uganda
Guinea-Bissau	Ukraine (including the territory of Crimea)
Heard and McDonald	United Kingdom
Hungary	Venezuela
India	Virgin Islands (British)
Iran	Virgin Islands (US)
Iraq	Wallis and Futuna.
Italy	Yemen
Latvia	Zimbabwe
Lebanon	



11.3 Appendix C | Risk core

In all risk sections, if one or more extremes are chosen, the whole section should be classified as extreme and senior management should be contacted before proceeding any further.

Risk Classification Time Frames for the re-review:

Shall be taken as guidance points and not as a mandatory rule.

SDD LOW RISK – 36 months to 60 months

CDD Medium – 18 months to 36 months

EDD High Risk – 12 months to 18 months

1. Customer Risk

Definitions:

Customer Risk - type of risk factor. If the risk factor type is not assessed, a low risk rating should be assigned.

Description - Description and variability. In each section, if more than 1 answer is applicable, please choose the answer carrying the highest risk.

Risk Score - assigning a point gradation to each risk level.

Customer Risk	Description	Risk Score
If the customer is under the sanction	Yes/No	YES - EXTREME CONTACT SENIOR MANAGEMENT AND MLRO NO LOW (16)
If the customer is a PEP	Yes/No	YES - EXTREME CONTACT SENIOR MANAGEMENT NO- LOW (16)
Customer's Source of Wealth Explained	● Extreme: - Source of Wealth unverified, - False declarations made, - Generated from a sanctioned country. ● High: - Have multiple sources of income (more than 3), - Gifts/Donations, - Income generated from VFA (non-regulated)	EXTREME – CONTACT SENIOR MANAGEMENT High (16) Medium (10) Low (5)



	● Medium: - Actual/Punitive damages awarded as a result of litigation (court of settlements), - Selling of Real Estate, - Profits and Dividends from a financial investment, - Investment of Private Securities, - Income generated from VFA (regulated) ● Low: - Employment, - Inheritance, - Winnings from a licensed entity, - Investment in Publicly Listed Securities, - Royalties - Rental Income,	
Duration of customer relationship	Less than 3 months - High 3 to 12 months - Medium More than 1 year - Low	High (16) Medium (10) Low (5)
Estimated Average bet size (per month)	0,00 - 10,00 USD - Low 11,00 – 50,00 USD - Medium 51,00 + USD - High	High (16) Medium (10) Low (5)
Multiple casino accounts or wallets (all websites within one company)	Yes/No	YES – HIGH (16) NO – LOW (5)
Total Score		
Classification		HIGH: 79 – 100 MEDIUM: 53 – 78 LOW RISK 0-52

2. Jurisdiction Risk

Definitions:

Jurisdiction - type of risk factor. If the risk factor type is not assessed, a low risk rating should be assigned.

Highest Ranked Jurisdiction - column displaying the country corresponding to the section in order from highest to lowest risk

Risk Score - assigning a point gradation to each risk level

Jurisdiction:	Highest Ranked Jurisdiction	Risk Score
Of Residential Address		HIGH (25) MEDIUM (17) LOW (8)
Of Nationality		HIGH (25) MEDIUM (17) LOW (8)
Of Place of Birth		HIGH (25) MEDIUM (17) LOW (8)
Of the IP address		HIGH (25) MEDIUM (17) LOW (8)
Total Score		
Classification		HIGH: 69 – 100 MEDIUM: 33 – 68 LOW RISK 0-32



3. Product Risk

Definitions:

TYPE OF GAME - type of risk factor. Type of game offered.

LOW/MEDIUM/HIGH - column displaying the value of the risk level to the type of game offered.

Risk Score - assigning a point gradation to each risk level.

If Product not being offered a low-risk score should be given:

TYPE OF GAME	LOW/MEDIUM/HIGH	Risk Score
Sportsbook	HIGH	HIGH (16) MEDIUM (12) LOW (6)
Virtual Sports	MEDIUM	HIGH (16) MEDIUM (12) LOW (6)
E-Sports	HIGH	HIGH (16) MEDIUM (12) LOW (6)
Casino – Slot Games	LOW	HIGH (16) MEDIUM (12) LOW (6)
P2P – Casino	HIGH	HIGH (16) MEDIUM (12) LOW (6)
Live Casino – vs House	MEDIUM	HIGH (16) MEDIUM (12) LOW (6)
Total Score		
Classification		HIGH: 73 – 100 MEDIUM: 37 – 72 LOW RISK 0-36

4. Transaction risk

Definitions:

Risk Type - type of risk factor. Type of the method of transaction being conducted. If the risk factor type is not assessed, a low risk rating should be assigned.

Description - Description and variability. In each section, if more than 1 answer is applicable, please choose the answer carrying the highest risk.

Risk Score - assigning a point gradation to each risk level.

Transaction Type	Description	Risk Score
Deposit/withdrawal method	High: -Cash - Prepaid card / vouchers - VFAS (CRYPTO CURRENCIES) - Online E-Wallets or all PSPs that allow customers to fund with cashor quasi-cash - third-party accounts or cards - Transfer of Funds BetweenGaming Accounts	HIGH: (33) MEDIUM: (22) LOW RISK (11)



	- Use of casino accounts (Withdrawal without Play) ● Medium: - Credit Card EU/EEA/SEPA/Visa/MasterCard - Online E-Wallets or all PSPs WHICH DO NOT ALLOW CUSTOMER TO FUND WITH CASH OR QUASI CASH ● Low: - Debit Card EU/EEA/SEPA/Visa/MasterCard - Digital Wallets (Apple/Google/Samsung pay)	
Withdrawal amount (per request)	\$0-\$2199 (Low) \$2200-\$9999 (Medium) \$10000(High)	HIGH: (33) MEDIUM: (22) LOW RISK (11)
Deposit amount (per session)	\$0-\$2199 (Low) \$2200-\$9999 (Medium) \$10000+(High)	HIGH: (33) MEDIUM: (22) LOW RISK (11)
Total Score		
Classification		HIGH: 67 – 100 MEDIUM: 34 – 66 LOW RISK 0-33

5. Interface Risk (Delivery channels) - ONLY ONE FACTOR

Definitions:

Risk Type - type of risk factor. Type, method, and interface of business relationship support.

Description - Description and variability. Only one factor is applicable.

Risk Score - assigning a point gradation to each risk level.

Risk Type	Description	Risk Score
Client interaction interface	NON-FACE-TO-FACE THROUGH AGENT	HIGH 100
	NON-FACE TO FACE - VPN	HIGH 100
	NON-FACE-TO-FACE THROUGH INTERMEDIARY	HIGH 100
	NON-FACE-TO-FACE THROUGH INTRODUCER/AFFILIATE	MEDIUM 50
	NON-FACE TO FACE DIRECTLY	MEDIUM 50
	FACE-TO-FACE – DIRECTLY	LOW 10
Total Score		
Classification		HIGH: 100 MEDIUM: 50 LOW RISK 10



Risk Classification	Total Score
Customer Risk	HIGH: 79 – 100 MEDIUM: 53 – 78 LOW RISK 0-52
Jurisdiction Risk	HIGH: 69 – 100 MEDIUM: 33 – 68 LOW RISK 0-32
Product Risk	HIGH: 73 – 100 MEDIUM: 37 – 72 LOW RISK 0-36
Transaction risk	HIGH: 67 – 100 MEDIUM: 34 – 66 LOW RISK 0-33
Interface Risk	HIGH: 100 MEDIUM: 50 LOW RISK 10
Total Risk Score	
Final Risk Classification	HIGH: 335 - 500 MEDIUM: 164 –334 LOW: 0 - 163

12. Senior Management Approval

Senior management has approved this AML compliance program in writing as reasonably designed to achieve and monitor our firm's ongoing compliance with the requirements the AML/CFT/CPF - regulations for landbased and online casinos, regulations of National Ordinance on identification when rendering services (NOIS) and National Ordinance on the reporting of unusual transactions (NORUT).