

AML/CFT Policies and Procedures

Surewin B.V

Table of Contents

CHANGE CONTROL	4
1. INTRODUCTION	5
1.1 PURPOSE	5
1.2 WHO DOES THIS MANUAL APPLY TO?	5
1.3 APPOINTMENT OF A MONEY LAUNDERING OFFICER AND COMPLIANCE OFFICER	6
2. WHAT IS MONEY LAUNDERING	6
2.1 STAGES OF MONEY LAUNDERING	6
2.2 HOW WE MIGHT BE ABUSED BY MONEY LAUNDERERS	7
2.3 WHAT IS FINANCING OF TERRORISM?	7
2.4 WHAT IS FINANCING OF PROLIFERATION OF WEAPONS?	8
2.5 TARGETED FINANCIAL SANCTIONS	8
3. LICENSING OBJECTIVES AND LEGISLATIVE REQUIREMENTS	9
4. RISK APPETITE OF SUREWIN B.V	9
5. THE RISK BASED APPROACH	10
5.1 GEOGRAPHY RISK	10
5.2 PRODUCT RISK	10
5.3 CLIENT RISK	11
5.4 DISTRIBUTION CHANNELS RISK	11
5.5 TRANSACTION RISK	12
6. BUSINESS RISK ASSESSMENT (BRA)	12
6.1 GEOGRAPHICAL RISK	12
6.2 CUSTOMER RISK	13
6.3 TRANSACTION RISK	14
6.4 PRODUCT RISK	15
6.5 DISTRIBUTION CHANNELS RISK	15
6.6 EMPLOYEE RISK	15
7. CUSTOMER RISK ASSESSMENT (CRA)	16
7.1 OTHER CONSIDERATIONS – SANCTIONS	17
7.2 OTHER CONSIDERATIONS – PEPs	17
7.3 OTHER CONSIDERATIONS – ADVERSE MEDIA	18
7.4 OTHER CONSIDERATIONS – PROBLEM GAMBLERS	18
7.5 OUR APPROACH	18
7.6 PLAYER RISK MATRIX	19
8. TECHNOLOGICAL DEVELOPMENTS RISK ASSESSMENT	20
9. CUSTOMER ACCEPTANCE POLICY (CAP)	20
10. CUSTOMER DUE DILIGENCE	22
10.1 INTRODUCTION	22
10.2 THE CUSTOMER DUE DILIGENCE (CDD) MEASURES	22
10.3 IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER	23
10.4 OBTAINING INFORMATION ON THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP	23
10.5 IDENTIFICATION AND VERIFICATION OF THE PLAYER	24
10.6 ON-GOING MONITORING	25
10.7 TIMING OF CDD MEASURES	28
10.8 ENHANCED DUE DILIGENCE	29

10.9 SIMPLIFIED DUE DILIGENCE	33
10.10 POLITICALLY EXPOSED PERSONS	33
10.11 APPLICATION OF CDD MEASURES TO EXISTING CUSTOMERS	39
10.12 THE TERMINATION OF THE BUSINESS	40
10.13 RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE	41
11. REPORTING OF UNUSUAL TRANSACTIONS	41
11.1 INTRODUCTION	41
11.2 RECOGNITION OF UNUSUAL TRANSACTIONS	42
11.3 REPORTING UNUSUAL TRANSACTIONS	43
11.4 AML/CFT REGISTERS	44
12. RECORD KEEPING	44
12.1 RETENTION PERIODS	45
13. NO CASH POLICY	45
14. EMPLOYEE SCREENING PROGRAM AND ONGOING EMPLOYEE TRAINING PROGRAM	45
14.1 EMPLOYEE SCREENING PROCESS	46
14.2 SECURITY FUNCTION	46
14.3 SYSTEM CONTROLS	46
14.4 TRAINING	47
15. EXTERNAL DATA REQUESTS	47
16. THIRD PARTY RELATIONSHIPS	48
17. AUDIT FUNCTION	48
18. BREACH OF THIS POLICY	48
SCHEDULE 1 - GLOSSARY	49
SCHEDULE 2 - UNUSUAL TRANSACTION REPORT (UTR) TEMPLATE	50
SCHEDULE 3 – PEP ASSESSMENT FORM	52
SCHEDULE 4 - SANCTIONS ASSESSMENT FORM	54

Change Control

Version	Name	Date
1.1	Craig Murugan	Date Prepared: 09/04/2024

1. Introduction

This Anti-Money Laundering and Counter-Terrorist Financing Policy and Procedure (the “Policy”) includes these Policies and Procedures in relation to: Anti-Money Laundering, Counter-Terrorist Financing (“CTF”), Politically Exposed Persons (“PEPs”), and Sanctioned Individuals and Companies. Consistent with international guidelines and relevant legislation, for the purpose of this document ‘Anti-Money Laundering’ should be read as ‘Anti-Money Laundering and Counter Terrorist Financing’ unless stated otherwise.

This manual seeks to provide guidance to the Due Diligence Obligations (“DDO”) in relation to the obligations of Surewin B.V and also comply with the obligations regarding regulations.

Law, Regulations and Rules

The Code of Criminal Law (Penal Code) of Curacao lays down the procedures for the prosecution of a money laundering offence as well as the measures for the confiscation of property upon a conviction of money laundering, measures for the freezing of assets when a person is charged with an offence of money laundering and measures for the issuance of an investigation and/or attachment order when a person is suspected of having committed an offence of money laundering.

The policies and procedures in this manual aim to comply with both the rules and guidance contained in, the NORUT and the NOIS which regulations themselves are referring to the Penal Code. In addition to these regulations the Central Bank of Curacao and Sint Maarten has introduced a comprehensive framework with provisions and guidelines to prevent and combat money laundering and terrorist financing (hereinafter: the “Provisions and Guidelines” or “P&G”). Curaçao - as a member of the FATF - has based these Provisions and Guidelines on, among others, the FATF recommendations.

Both the NORUT and the NOIS are applicable on entities which are offering the possibility to take part in offshore hazard games (online gambling) in or out of Curaçao which is the case for the Surewin B.V

This manual is being issued and has been approved by Surewin B. V’s Board of Directors and incorporates Surewin B.V policies and procedures that must be adhered to prevent opportunities for money laundering in relation to Surewin B.V and its activities.

1.1 Purpose

To prevent the customers from exploiting Surewin B.V for purposes of money laundering and terrorist financing, Surewin B.V is fully committed to complying with the laws and regulations of its licensing bodies. The purpose of this manual is to establish the policy, procedures and measures designed to reasonably ensure that money laundering and terrorist financing transactions are prevented from occurring or are detected on a timely basis by Surewin B.V

1.2 Who does this Manual apply to?

This manual applies to all employees, relevant officers all customers who have opened real-money customer accounts with Surewin B.V

There are no exceptions to this.

This manual should be followed at all times and non-compliance will be treated in an extremely serious manner.

If at any time it is impractical to follow the provisions of the manual, written permission to deviate from the procedures must be obtained from the board of directors of and the MLRO, before any action is taken.

1.3 Appointment of a Money Laundering Officer and Compliance Officer

Surewin B.V has appointed **XCM** to receive notifications of internal reports of knowledge or suspicion of ML or FT, known as UTRs. This person is commonly referred to as the **MLRO** and:

- Is sufficiently senior and has sufficient expertise and authority.
- Has a right of direct access to the officers of Surewin B.V; and
- Has sufficient time and resources to properly discharge the responsibilities of the position.

The MLRO can be contacted at: cnagtegaal@xcm.cw

The MLRO is responsible for the UTR reporting process and handling of UTRs, as well as assisting with CDD/EDD requirements for customers and review / approval of high-risk customers.

Surewin B.V has appointed **Craig Murugan** as the Compliance Officer.

The Compliance Officer is responsible for reviewing the contents of this manual on an ongoing basis to ensure that procedural and or regulatory or legislative amendments are reflected. Any amendments are approved by the Directors and MLRO.

2. What is Money Laundering

AML is the acronym for anti-money laundering. Money Laundering is the attempt to conceal or disguise nature, location, source, ownership, or control of illegally obtained money.

In practice, money laundering covers all procedures to change the identity of illegally obtain funds (including cash) so that they appear to have originated from a legitimate source. Money laundering has three coming factors:

- Criminals need to conceal the true ownership and origin of the money.
- They need to control the money; and
- They need to change the form of the money.

As a regulated firm, Surewin B.V is subject to various AML regulations. These require the firm to put in place systems and controls to prevent and detect money laundering.

2.1 Stages of Money Laundering

2.1.1 Placement - During the first stage of money laundering, illegal monies are introduced into the financial system e.g., through deposits in a bank account and purchase of money vouchers. Illegal proceeds are easier to detect in the placement stage when the physical currency enters the financial system.

2.1.2 Layering - Illicit proceeds are separated from the source by creating complex layers of financial transactions designed to disguise the audit trail and provide anonymity.

2.1.3 Integration - If the layering process has succeeded, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing to be normal business funds. Thus, this stage provides apparent legitimacy to criminally derived funds.

The purpose of these stages:

Converting criminal property from one form into another in order to Conceal its origin, destination, ownership etc., but whilst allowing the criminal to Control it or retain the benefit of it.

It disconnects any easily traceable link between the criminal and the property.

We must remember that it is more likely to involve more than just the three steps noted above, an effective laundering operation can stretch over multiple jurisdictions, multiple layers coming into and out of the financial system and be realized as various assets.

Each additional step provides an additional disconnect from the original offence for the criminal.

We must also remember that it is unlikely that we would be used for all stages - rather than trying to think which phase of the model has occurred, you should ask yourself “Do I know, suspect or have reasonable grounds to suspect that the property in question is criminal property?”

2.2 How we might be abused by money launderers

eGaming represents one of the largest economic sectors and has been assessed as presenting a medium risk for abuse of ML. The nature of operations means business is conducted non face to face which presents various risks.

The three-stage traditional model as described above is far simpler than in reality. To demonstrate the vulnerabilities Surewin B.V needs to consider the wider picture:

Generation – The illicit funds are generated from illegal activities e.g., tax evasion, corruption, fraud, drug dealing.

- Consolidation – Those funds are deposited into a bank account.
- Placement – The funds are deposited into a player’s account.
- Layering – Small amounts are used to gamble.
- Realisation – The balance of the account is withdrawn showing the origin being a legitimate source successfully disconnecting themselves from the original property.

2.3 What is Financing of Terrorism?

Terrorism financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

Stages of Terrorist Financing are as follows:

- Collection – funds are often acquired through seeking donations, carrying out criminal acts or diverting funds from genuine charities.
- Transmission – where funds are pooled and transferred to a terrorist or terrorist group.
- Use – where the funds are used to finance terrorist acts, training, propaganda etc.

Like the traditional three phase model for ML, this model is rather simplistic and outdated. Rather than trying to think which phase of the model has occurred, you should ask yourself “Do I know, suspect or have reasonable cause to suspect that the property in question is terrorist property?”

We must remember that FT differs from ML as the funds are not necessarily obtained by illegitimate origins.

The Consequences of ML, FT and PF

ML/FT/PT can have serious negative consequences for the economy, national security and society in general. Some of the consequences may include:

- reputational damage from being perceived as being a haven for money launderers and terrorist financiers, leading to legitimate business taking their business elsewhere.
- attracting criminals including terrorists and their financiers to move to or establish new business relationships within the jurisdiction.
- damaging the legitimate private sector who may be unable to compete against front companies.
- weakening of financial institutions who may come to rely on the proceeds of crime for managing their assets, liabilities and operations, plus additional costs of investigations, seizures, fines, lawsuits etc.
- economic distortion and instability.
- increasing tax rates due to the loss of tax revenues following tax; or
- increased social costs to deal with additional criminality such as policing costs or hospital costs for treating drug addicts. Reputational damage and attraction of criminals amongst others.

2.4 What is Financing of Proliferation of weapons?

Proliferation of weapons of mass destruction (“WMD”) can be in many forms but ultimately involves the transfer of export of technology, goods, software, services or expertise that can be used in programmes involving nuclear, biological or chemical weapons and their delivery systems (e.g., long range missiles). Proliferation of WMD financing is an important element and, as with international criminal networks, proliferation support networks use the financial system to carry out transactions and business deals.

2.5 Targeted Financial Sanctions

Sanctions are prohibitions and restrictions put in place with the aim of maintaining or restoring international peace and security. They can:

- Limit the provision of certain financial services;
- Restrict access to financial markets, funds and economic resources.

They generally target specific individuals or entities, or particular sectors, industries or interests. They may be aimed at such people and things in a particular country or territory, or some organisation or element within them.

Sanctions are generally imposed to:

- Coerce a regime, or individuals within a regime, into changing their behaviour (or aspects of it) by increasing the cost on them to such an extent that they decide to cease the offending behaviour;
- Constrain a target by denying them access to key resources needed to continue their offending behaviour, including the financing of terrorism or nuclear proliferation;
- Signal disapproval, stigmatising and potentially isolating a regime or individual, or as a way of sending broader political messages nationally or internationally; and/or
- Protect the value of assets that have been misappropriated from a country until these assets can be repatriated.

Financial sanctions apply within the territory of the Curacao and to all Curacao persons (i.e. individuals and legal entities), wherever they are in the world. All individuals and legal entities who are within or

undertake activities within the Island's territory must comply with the financial sanctions that are in force. For example, this includes an operational business such as Surewin B.V

In order to comply with our obligations in line with the above, Surewin B.V undertakes screening upon first deposit via NameScan and thereafter ongoing screening throughout the duration of the customer relationship against relevant sanctions lists.

Where a potential match is identified, additional information and EDD will be obtained in order for the validity of that potential match to be considered. Any potential match will result in the customer's account being immediately frozen and a Sanctions Assessment will be sent to the MLRO.

Any match found to be a false positive will be recorded in the Sanctions Monitoring Register. A copy of the Sanctions Assessment form is attached to this Manual as Schedule 4.

If a match is positive the account will remain frozen, the relationship terminated, and the MLRO will submit the necessary report to the FIU. If the account holds a balance the MLRO will advise where they should be sent following confirmation / consent from the FIU. The customer will be marked as a prohibited player so an account cannot be registered in the future.

3. Licensing Objectives and Legislative Requirements

- Surewin B.V will continually review and revise its policies and procedures considering relevant legislation, regulation, and industry guidance/learning.

4. Risk appetite of Surewin B.V

- Risk appetite is an expression of the maximum level of risk that Surewin B.V is prepared to accept to achieve our business objectives.
- Our risk appetite statement translates our strategy into measurable short to medium term targets and thresholds across material risk categories and enables intra-year performance monitoring and management, which aims to identify optimal growth options considering the risk involved and the allocation of available capital resources to drive sustainable performance.
- The board and the executive management team use a combination of different and complementary skills to assess the risks facing the business. In determining its risk appetite,

The board considers:

- Updates provided by senior management on key strategic, and operational matters.
- Significant matters that have been reserved for the board.
- Risk assessments
- The reports of the internal auditors

5. The Risk Based Approach

A risk-based approach describes the process to which Surewin B.V ensures that the systems and controls are based on the risk of money laundering Surewin B.V is facing. The risk-based approach is introduced to promote a move away from a “one size fits all” approach to anti-money laundering procedures. By identifying and assessing the money laundering risks, Surewin B.V can take the best steps to mitigate and monitor those risks.

Surewin B.V has a robust AML Platform, to enhance the accuracy and reliability of our CRA process.

The platform automates risk events and reduces the risk of human bias, ensuring a more consistent and reliable approach to assessing customer risk.

Some of the advantages:

- Monitors ongoing risk automatically and deliver alerts whenever human review is necessary.
- Streamlines investigation complexity for increasing caseloads
- Standardised inconsistent processes to meet regulatory requirements
- Removed bias from player risk assessments
- Fulfills documentation requirements for audits
- Ensures document validity

5.1 Geography Risk

An assessment is carried out and an internal scoring is assigned; accordingly, such risk level will be then reflected as part of the client’s risk assessment.

5.2 Product Risk

Surewin B.V provides casino products and currently does not seek to delve into products or services which are deemed to be higher in risk, which makes such products more attractive for illicit activity or criminal intent.

a. Transparency

The product in no way allows or permits any anonymity from the user, cases where there is pooled betting or there is suspicion that a player is playing on behalf of somebody else shall be immediately considered as the beneficial owner.

b . Complexity

The transactions described under transaction risk have been mitigated to a money-in-money system, meaning that the method of payment used shall be the same method the customer may use to withdraw funds. The client may have a number of payment methods through which all needs to be verified to withdraw the funds. The product is therefore limited, and no multiple parties or jurisdictions are allowed.

c. Value and Size

The value and size of the product shall be carried out through methods that have a money trail, i.e. methods of electronic payment only the product shall allow high value transactions only thought the

verification of the beneficial owner and holding sufficient evidence that the funds are obtained legitimately and such may only be allowed over the course of the business relationship. The product has limits and thresholds through which, although allowed, will prompt the client to present a level of due diligence which is calculated as a percentage of the total net income of the said beneficial owner. The product holds no capping in place although alerts are in place which block the beneficial owner from transacting further unless an explanation and verification has been provided.

5.3 Client Risk

Understanding the risks that may arise from the above factors, Surewin B.V has taken up the development of sound risk management practices, to help assist the officers involved in the process and tools to manage the risk posed by the threats of money laundering, funding of terrorism or other illicit activity.

The mandatory high risk players shall be as follows:

- PEP
- High net worth individuals
- Reactivated accounts after long periods of dormancy
- Suspicious transaction pattern
- Multiple revenue streams
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Customers with irregular income streams;
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Income originating from a high-risk jurisdiction

Additionally, the following risk factors are taken into account when assessing the customer risk of a player:

- Customer Verification: KYC Status
- Account block reason;
- Employment status;
- Occupation;
- Adverse media;
- PEP + High Risk Countries

5.4 Distribution channels risk

The distribution channel risk interface of Surewin B.V is that of non-face to face, due to the nature of the said business face-to-face, with sufficient technology in place to mitigate such risks.

- Non-Face-to-Face - Deposits =>2000 --- High Risk
- Non-face-to-face & Deposits <2000 --- Standard Risk

5.5 Transaction Risk

It is important to note that due to the current anti-money-laundering and funding of terrorism regulations, the player may deposit money only to play and use our services. Likewise, the player may only withdraw winnings and not the funds deposited into the account without any game play.

Surewin B.V is not a financial institution or credit institution and does not grant interest on deposits. In any case, Surewin B.V reserves the unlimited right to apply certain restrictions on the payment methods if selected.

In terms of the customer risk assessment, the following risk factors are considered to assess the transaction risk of all players upon reaching:

- 2000 EUR threshold in deposits
- Total Deposits in the last 12 months more than 30% of the average Salary;
- E-Wallets - EUR 500 or more deposits in the last 2 months;
- More than 3 payment instruments used in the last 72 hours;
- Threshold EUR 10k in 7 days;
- Threshold EUR 15k in 30 days.

6. Business Risk Assessment (BRA)

- Surewin B.V has conducted an AML and CFT business risk assessment (the “BRA”), which will be reviewed on an annual basis, and as needed.
- The Risk Assessment seeks to identify the potential risks to Surewin B.V in the following areas: geographical risk, customer risk, payment risk, product risk, interface risk and employee risk.
- The Risk Assessment also takes account of risk factors related to transactions and delivery channels, as part of the analysis of payment risk and employee risk. Surewin B.V develops and implements proportionate, risk-based procedures and processes, designed to address the risks identified in the Risk Assessment.
- A record will be kept detailing how and why these policies and procedures have been amended and, where appropriate, upgraded from time to time.
- In carrying out the BRA, the management must keep the following factors in mind:

6.1 Geographical Risk

Location of customer

We take the necessary measures to identify the location of the player or prospective player. This is to minimize the risk of facilitating illegal gambling in countries where it is not allowed and to ensure that gambling is not offered to prohibited jurisdictions in accordance with our Terms and Conditions.

Reports are reviewed daily to identify customers that have accessed the site from any High- Risk Jurisdictions.

This risk is mitigated by having measures in place to check the user's IP address location and by removing prohibited jurisdictions from the countries' list during the registration process. In addition, we have taken measures together with our Payment Service Providers (PSPs) to ensure that we do not accept deposits from restricted or high-risk territories, as evidenced by their IP address or their Bank Identification Number ("BIN").

Jurisdictional risk factors

Players from countries that are deemed "High-Risk Jurisdictions subject to a Call for Action" and "Jurisdictions under Increased Monitoring") are not accepted due to the high risk they represent.

Reports are reviewed daily to identify customers that have accessed the site from any High-Risk Jurisdiction.

To mitigate this risk, the country's list of registration processes is restricted to make available only those countries that can register an account. Other restricted or prohibited countries are removed from the registration process.

Other factors used in determining Geographic Risk of a customer are:

- Countries subject to sanctions, embargoes or similar.
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures.
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

6.2 Customer risk

It is critical to determine the potential money laundering and/or terrorist financing risks posed by our players to develop and implement an effective overall risk-based framework.

Based on different criteria, Surewin B.V will be able to determine whether a particular player poses a higher risk and the potential impact of any mitigating factors in that assessment.

Through the application of risk variables, Surewin B.V will be able to mitigate the risks posed by the threat of being used for money laundering and/or terrorist financing.

A key risk mitigation strategy is ensuring that Surewin B.V holds adequate customer due diligence ("CDD") measures on its players.

Surewin B.V needs to be aware of its players overall spending by monitoring their activity and transactions as this information is important to determine whether the players are gambling with their own means, to identify any signs of problem gambling, or also to determine whether the activities/transactions are suspicious in terms of money laundering and/or terrorist financing.

Surewin B.V is currently using a risk score model to give a risk score to the players on its database. Players are categories in 3 main categories: Standard Risk, Medium Risk, and High Risk.

6.3 Transaction Risk

Changes to financial institution accounts

Players may hold several accounts with financial institutions, and they may wish to change which of these accounts they use in casinos. Given the risk of identity fraud, checks and limitations need to be in place on such account changes.

Surewin B.V has limited the number of cards that are permitted on a player's account i.e., 5 cards are allowed where a player may deposit with limited use to electronic cards issued by their financial (banking) institutions.

Changing depositing accounts regularly increases the risk that customers will place and layer criminal proceeds through gambling transactions. This risk is mitigated by linking winnings pay-outs with how the player deposited to carry out gambling transactions. Hence, where it is feasible, funds will be returned to players to the same source to limit the opportunity for a money launderer to layer the proceeds of criminal activity. The closed loop system should always be preferred and where the closed loop is broken, the transactions should be scrutinized.

Surewin B.V will allow the player to select a new bank card/account if prior to withdrawal, full KYC documentation has been received and that Surewin B.V has confirmed beyond a reasonable doubt that the identity of the card or account holder matches that of the player's account.

Payment Gateway Stage - The payment gateway that is used by Surewin B.V is integrated with 3D-Secure and Capture-Delay from its end that is at deposit stage. These mechanisms are intertwined and provide Surewin B.V with the first layer of protection against fraudsters and chargebacks.

Payment Methods:

Card payments - Copies of all debit/credit cards registered and used in the player's account.

These copies must display the player's signature together with the first six and last four digits of the card itself. For the player's own security and safety, players should block out the security number at the back and the middle digits in the front of their card.

Wallets - A screenshot of your wallet account showing the player's email address/account number and personal account information.

Bank Statement - A bank statement issued in the last 3 months for the player's bank account. This should include the player's bank name, bank account number, IBAN number and BIC code. All four corners of the statements are to be visible. The statement may be a hardcopy or a PDF.

Pre-paid vouchers - Players may use cash to purchase pre-paid vouchers. Hence, these pose a high money laundering risk as the purchaser of the vouchers might not be legitimate and it will be difficult to perform the same level of cross reference checks on some types of pre-paid vouchers as could be used in cases of financial institutions accounts. Especially because pre-paid vouchers are only used for depositing purposes.

To mitigate this risk, Surewin B.V produces reports specific to pre-paid vouchers to monitor and review the top depositors using these methods per week/month/year.

Players using vouchers are assigned a high-risk score. Should a player use pre-paid vouchers and

less risk deposit methods, the player is nonetheless assigned a higher risk, irrespective of the frequency and amount deposited through prepaid vouchers.

Inter account transfers - Transferring funds from one player to another player is strictly prohibited. This is also stated in our Terms and Conditions, which players are obliged to adhere to, to be able to register and access their gambling account. This limitation is in place to prohibit third parties buying existing player accounts to carry out ML.

6.4 Product Risk

Product risk includes the consideration of the vulnerabilities associated with the gambling products offered by Surewin B.V

Given that Surewin B.V primarily offers RNG Slots, the product risk is considered low. There are certain games where risk is hedged and constant high value playing on these types of games (such as roulette) only immediately after a deposit is made should they be scrutinized. Surewin B.V is not offering **Poker** or **Sport Betting** that is usually considered high risk. As a result, the management believed that the inherent product risk is marginal.

6.5 Distribution channels risk

The distribution risk is the risk arising from how Surewin B.V interacts with the customer and the channels it uses to provide a given product or service. Interacting with customers on a non-face-to-face basis need not be considered as automatically presenting a high risk of ML/FT.

The implementation by a subject person of technological means within its systems to address the risk of impersonation or identity fraud would significantly reduce the inherent risk arising from this form of interaction with customers.

Given that Surewin B.V operates an online casino where interaction with the customer takes place on a non-face-to-face basis, there will always be an element of inherent interface risk to AML and FT. Surewin B.V, however, takes several measures to mitigate this inherent risk, making sure that the residual risk is in line with its Risk Appetite. The measures and controls in place to address the inherent risk of identity fraud or impersonation include:

- Surewin B.V has a report in place that checks whether different user IDs were created using the same IP address.
- All players are asked to fill in a detailed registration form, so that they can be duly identified.
- Players' Identities are verified on a risk-sensitive basis.

6.6 Employee Risk

It is not only customers that pose a risk of ML/TF, but employees can also pose a risk to the business either due to lack of training or if such individuals would abuse the system for their own gain.

To safeguard against this risk Surewin B.V makes sure that all the employees involved in AML attend

at least one annual training session on the topic. Registers are kept on record to track the progress of training within the team. The AML policy is saved in a central database that is accessible by all the employees. New employees are encouraged to read the AML policy irrespective of the position held to make sure they are aware of the policies within Surewin B.V

7. Customer Risk Assessment (CRA)

Surewin B.V must carry out a CRA as soon as reasonably practicable after entering into an ongoing customer relationship and that risk assessment must estimate the risk of ML/FT/PF posed by the player. The assessment must be recorded and regularly reviewed to ensure it remains up to date.

Our CRA is undertaken in line with our BRA and the relevant risk factors it identifies as well as:

- the value of funds deposited;
- the jurisdiction of participant;
- the source of funds deposited;
- any other relevant matter brought to the attention of Surewin B.V during the account opening process for the participant;
- any relevant supervisory or regulatory guidance;
- the legal nature of the business participant.

Factors that pose a higher risk of ML/FT/PF

- Some factors result in a player posing a high risk jurisdiction.
- Being subject to a warning in relation to AML/CFT issued by a competent authority.

Any player identified as having any of the above two risk factors will be high risk and therefore subject to EDD. For their account to be approved for play, their assessment must be signed off by a Director.

Factors that *may* pose a higher risk of ML/FT/PF

Some factors may result in a player posing a higher risk of ML/TF/PF, these are:

- activity in a jurisdiction our company deems to be higher risk of ML/FT/PF;
- circumstances that by their nature present an increased risk of ML/FT/PF;
- a player that is a PEP;
- a player that is a HNWI;
- persons performing prominent functions for international organisations;
- players that are sporting professionals betting on sports;
- players that use multiple sources to fund their gambling activities.

The risk factors above are considered in the application of the CRA as well as any appropriate mitigation. Such mitigation must be demonstrated and recorded. Where a player presents as higher risk, EDD will be applied, and their assessment must be signed off by a Director.

Surewin B.V takes a holistic view of the ML/FT/PF risks identified that together determine the level of ML/FT risk associated with an area of the business including the location of a player meaning an isolated risk factor does not necessarily make a relationship a higher risk category.

When assessing ML/FT/PF risk, Surewin B.V weighs risk factors to make an informed judgement.

7.1 Other considerations – Sanctions

Where a potential match is identified, additional information and EDD will be obtained in order for the validity of that potential match to be considered. Any match found to be a false positive will be recorded in the Sanctions Monitoring Register.

Any positive match will result in the players account being immediately terminated. They will be advised via email that they have been unsuccessful in the registration process. Consideration will be given to making a UTR in line with the reporting procedures detailed below.

7.2 Other considerations – PEPs

Any participant that is identified as a PEP during screening will continue to have an inoperative account whilst EDD processes are applied.

The Risk team will advise the participant that their account is under review whilst EDD checks are being completed, and they will request the following:

- Additional measures to verify identity;
- Additional measures to verify address.

In addition, EDD will always include establishing the participant's SOW which could include:

- Details of employment history or a CV to cross reference;
- Copies of pay slips;
- Confirmation from employers;
- Copies of documents to demonstrate inheritance.

The participant will have **30 days** to provide this information. If it is not provided within that time the account will be closed by the relevant Risk staff members, who will raise an internal UTR to the MLRO. Consideration will be given by the MLRO as to whether a UTR is required to be made to the FIU.

Once the requested information is received the MLRO will conduct additional research using various platforms available to them. In addition, the MLRO may request further due diligence, but this will be decided on a case by case basis.

Any participant that is classified as a PEP but an acceptable risk and approved in line with the parameters will be classified as a higher risk player and subject to enhanced monitoring, but their account will be allowed to continue if all requests are met.

Enhanced monitoring will include review of every deposit and withdrawal as well behaviour / patterns, with any adverse information being reported immediately to the MLRO.

If upon receipt of enhanced due diligence, it is determined that the potential PEP match is a false positive, the Risk team will detail their findings within the back office setting their reasoning.

The Compliance Officer will review all discounted PEP matches during ongoing monitoring to ensure they have been documented adequately.

7.3 Other considerations – Adverse Media

Any participant that is identified as being the subject of adverse media during screening will continue to have an inoperative account whilst EDD processes are applied. Steps will be taken to confirm the media relates to the participant, or not. Each case will be assessed on a case by case basis and, where necessary, referred to the MLRO who will recommend the appropriate steps which can include conducting in depth searches within the public domain.

When potential matches cannot be discounted the Risk team will advise the participant that their account is under review whilst EDD checks are being completed, and they will request the following:

- Additional measures to verify identity.
- Additional measures to verify address.

In applicable circumstances EDD can include establishing the participant's SOW.

Each case will be assessed on a case-by-case basis by the MLRO who will recommend the appropriate risk rating of the participant.

7.4 Other considerations – Problem Gamblers

Any participant that is: -

- Listed as a problem gambler or
- Previously excluded from the site

will automatically have their account closed. Depending on the circumstances of the individual and their account the MLRO will consider if there is cause for suspicion and if so, will take the appropriate action.

7.5 Our Approach

All participants must create an account on the platform. The following information is required to create an account:

- Full name;
- Residential address;
- Country of residence;
- Date of birth.

Any anonymous or fictitious names will result in failure to use an account, which is detected by manual review of all newly registered customers on a daily basis. A Newly Registered Accounts report is generated daily for the previous day's registrations for review and any required action. Should any be missed, they will be identified during the identity verification process.

7.6 Player Risk Matrix

Following in-depth consideration of the preceding factors by Surewin B.V senior management the following matrix details Surewin B.V AML/CFT approach to player risk.

Action	Nature of participant	Jurisdiction	Source of Funds	Transaction size
Standard	Individuals with no screening hits	Full FATF AML/CFT Compliance	Consistent payment facility in name of player	Deposit <€2,000
Medium <i>(A player must meet two of the criteria to be considered medium risk)</i>	Individuals with some adverse media within the public domain, not relating to financial crime or gambling	Not subject to FATF's ongoing monitoring process.	Two changes in payment facility in name of player	Cumulative Deposit or withdrawal >€15,000
High	- Individuals with criminal or adverse gambling information within the public domain - PEP or PEP by association	- Countries which have strategic AML/CFT deficiencies - Countries which have strategic AML/CFT deficiencies as determined by FATF and other resources	More than two change in payment facility in name of player	Cumulative Deposit or withdrawal >€30,000
PROHIBITED	Business participants	Closed / blocked jurisdictions	Cash or payment facility not attributable to player	Dynamic – defined by senior officers

Following the risk assessment participants will be identified as either:

- Standard
- Medium
- High

The risk matrix particulars are applied to the settings within the back office.

The relevant level of CDD will then be applied to each participants account and reviewed on an ongoing basis as part of the monitoring procedure.

All high-risk customers must upload KYC that is commensurate with their risk rating. Whilst awaiting KYC documentation, the ability to deposit and/or withdraw funds is frozen. The ID documents must include a clear photograph and their date of birth; this information is then analysed by the Surewin B.V Risk team.

Surewin B.V's Risk Team provides the following services in relation to customer on boarding:

- Customer Service;
- Fraud / Risk Management Service.

All results are available to view in the Back Office portal and can be accessed by MLRO and Directors at any time. Reports can be generated to detail the results of verification and screening.

8. Technological developments risk assessment

When implementing new technology into the business, Surewin B.V will ensure that appropriate measures are taken to address, if required, any AML or CTF risk that might be presented by the new technology.

The assessment is revisited:

- Whenever a new product is developed;
- A new delivery mechanism becomes available;
- A new business practice emerges, in particular every time money and technology come together in a new way or
- A new technology is used to deliver new or old services.

This assessment serves to determine whether the innovation creates a weakness that can be exploited by money launderers or those seeking to finance terrorism. Where risks are identified, measures must be taken to mitigate the risks.

It is recognised that the development of new technologies is a fluid process and therefore all risk assessments will be prepared in advance of integration and revisited regularly.

A register of all Technology Risk Assessments and individual assessments are maintained in order to demonstrate its basis and how they are reviewed.

9. Customer Acceptance Policy (CAP)

The Client Acceptance Policy (hereinafter the “CAP”), following the principles and guidelines described in this manual, defines the criteria for accepting new Clients and defines the Client categorization criteria which shall be followed by Surewin B.V and especially by the employees which shall be involved in the client acceptance and processing procedure for the provision of the services.

The scope of the CAP is to:

- Manage any risk that Surewin B.V may be exposed to through the provision of its services to customers.
- To prevent Surewin B.V from being used, intentionally or unintentionally, for money laundering and/or terrorist financing purposes; and
- To identify customers who are likely to pose a higher-than-average risk.

Surewin B.V is to outrightly refuse those instances where the client does not fall within the risk appetite or have been deemed though the analysis of the risk assessment to be of a higher risk towards Surewin B.V provide for the identification of the different type of customers, individual and/or corporate, that are likely to pose a higher-than-average risk or fall Surewin B.V appetite.

After the identity verification a risk profile is formed based on the behavioral pattern of the customer. This behavioral pattern is examined through the transaction activity and the type of game- play. After the behavioral pattern is analyzed, every customer is given an internal classification as defined by the client risk assessment. If suspicious behaviour is observed, evidence will be recorded on the customer profile, and enhanced customer due diligence is applied.

Surewin B.V has a medium-risk appetite, which can be managed through robust controls and risk mitigation strategies. These strategies include not only the application of Enhanced Due Diligence (EDD) based on risk level criteria and procedures within the Organisation but also identifying risks associated with products and continuously monitoring and strengthening controls through the business risk assessment process.

Those clients who do not comply with the due diligence procedures or who are deemed to try to bypass such shall not fall within the CAP also consider risks within the business risk assessment. Those clients who engage in wrongful activity or trigger any of the established rules within Surewin B.V set-up shall be reviewed for malicious practice and if intent is established such individuals or companies are not considered to be within the acceptance limits of Surewin B.V

The above section provides details of those situations in which Surewin B.V will outrightly refuse. The CAP shall also be predominantly determined by the risk assessment carried out on behalf of an individual. This document in its entirety shall be the basis for determining upon completion of the documentation for all clients whether the client will be within the risk appetite of Surewin B.V

Unacceptable Clients

The following list predetermines the type of Clients who are not acceptable or who operate within the lines of business as indicated for establishing a Business Relationship or an Occasional Transaction with Surewin B.V. The following lists are those customers for whom Surewin B.V will not engage in a business relationship or occasional transaction. The list has been compiled throughout the operation of Surewin B.V and is not exhaustive. The list hereunder shall be updated on instances where the board of directors deems new and evolving lines of business and a high and unacceptable risk towards Surewin B.V such as mentioned above shall be raised to senior management for approval of the decline and an analysis will also be made in the case where an UTR is to be raised:

- Clients who fail or refuse to submit the requisite data and information for the verification of his identity and the creation of his economic profile, without adequate justification.
- Clients who have been convicted of criminal acts either by the relevant courts of Curacao or in any other part of the world.
- Clients who are sanctioned
- Client with intent to commit ML/FT
- Clients who are involved in business activities which are illegal, unethical or involve actions which are contrary to public order or moral standards.
- Clients who are sanctioned by international or governmental organisations.
- Sanctioned individuals and entities.
- Applicants for business involved in child pornography.
- Applicants for business involved in illegal drug paraphernalia.
- Applicants for business involved in pyramid sales.
- Applicants for business involved in the production or trade in radioactive materials and or arms of mass destruction.
- Applicants for business involved in the production or trade in weapons and munitions or spare parts of war related vehicles.
- Applicants for business involved in production or activities involving harmful or explosive forms.
- Applicants for business involved in forced/harmful child labour activities.
- Applicants for business involved in any form of counterfeit goods.

- Verification or reason to believe that funds were obtained illegally or are derived from illicit purposes.

10. Customer Due Diligence

10.1 Introduction

Surewin B.V adheres to and complies with “Know You Customer” principles, which aim to prevent financial crime and money laundering through client identification and due diligence.

Surewin B.V may at any time ask for any KYC documentation it deems necessary to determine the identity and location of a user.

Surewin B.V will restrict the service, payment, or withdrawal until identity is sufficiently determined, or for any other reason in our sole discretion based on the legal framework.

We take a risk-based approach and perform strict due diligence checks and ongoing monitoring of all clients, customers, and transactions.

As per the Money Laundering Regulations, we utilize 3 stages of due diligence checks, depending on the risk, transaction, and customer type.

- SDD – Simplified Due Diligence is used in instances of extremely low risk transactions that do not meet the required threshold.
- CDD – Customer Due Diligence is the standard for due diligence checks, used in most cases for verification and identification.
- EDD – Enhanced Due Diligence is used for high-risk customers, large transactions or unusual cases.

10.2 The Customer Due Diligence (CDD) measures

CDD measures are not in principle applicable until the two thousand Euro (€2,000) threshold is reached. However, to ensure the proper functioning of AML/CFT controls, a minimum level of CDD measures prior to the said threshold being reached is applied. Thus, simultaneously with the opening of an account, Surewin B.V identifies the customer by collecting the personal details which are set as the minimum applicable in case of low-risk scenarios.

Clients must first register with us and open an account in order to be able to place bets and deposit money:

- They are only allowed to have one account per client, which must be registered personally.
- They are only allowed to create one account on the Website that we supply. If a client tries to open more than one account, all of their bets may be forfeited, and all of their accounts may be blocked or cancelled. Any duplicate / multiple account may be terminated at any moment by Surewin B.V
- Surewin B.V conducts verification checks on clients, and accounts that are found to have provided incorrect or misleading information may be blocked or closed.
- Accounts must contain correct information to allow for the proper risk assessment of the player therefore fictitious, anonymous and numbered accounts are prohibited.
- Documents provided to verify an address should not refer to PO Boxes or ‘care of’ addresses.

Customers who do not reach the CDD threshold of two thousand Euro (€2000) are to be identified, by keeping the details usually obtained through our registration process. These details include:

- a) Full name;
- b) Residential address;
- c) Country of residence;
- d) Date of birth.

Deposits and payments details are reviewed and verified to ensure they match the personal data submitted by the customer, preventing the customer from receiving a deposit or making a payout from or to a third party. Deposits and payments details that are verified, depending on the method of payment used, may include name, date of birth and/address.

Customers not meeting the CDD threshold of two thousand Euro (€2,000) are nonetheless monitored and if an unusual deposit or game activity is noted, they are nonetheless subjected to KYC.

Surewin B.V also ensure that any first withdrawal is subjected to KYC.

10.3 Identification and verification of the Beneficial Owner

Surewin B.V does not support - and the system does not allow - the registration of business participants, organisations, foundations, legal arrangements or individuals acting on behalf of organisations as customers. The registration process will only facilitate the application of an individual. Should an individual be found to be acting on behalf of an organisation, their account will be immediately frozen and suspended.

10.4 Obtaining information on the Purpose and Intended Nature of the Business Relationship

As part of the Customer Due Diligence (CDD) process, Surewin B.V will obtain and assess information regarding the **purpose and intended nature** of the business relationship at the time of account opening or onboarding.

This includes understanding:

- The **expected types and volume of activity**.
- The **source of funds and source of wealth**, where applicable.
- The **customer's business or occupation**, and how it relates to the relationship.

This information helps determine the customer's risk profile and ensures appropriate ongoing monitoring. The level of detail obtained will be proportionate to the assessed risk and the nature of the relationship.

The following measures will be implemented:

- **Customer Profiling:** Information such as occupation, source of funds, gaming preferences, and expected transaction volumes will be collected during registration or account creation.
- **Enhanced Due Diligence (EDD):** For high-risk customers (e.g., VIPs, foreign nationals, PEPs), additional verification and documentation of source of wealth will be required.

- **Transaction Monitoring:** Actual behaviour will be monitored and compared with expected patterns to detect inconsistencies.
- **Loyalty Program Data:** Customer relationship data from loyalty programs will be reviewed to assess transaction history and gaming behaviour.
- **Risk-Based Approach:** Each customer will be assigned a risk rating to determine the appropriate level of due diligence and monitoring.
- **Ongoing Reviews:** Customer profiles will be periodically updated, especially when significant changes in behaviour are observed.
- **Staff Training:** Employees will be trained to identify and document the purpose of a customer's relationship with the casino and to escalate concerns appropriately.

These measures ensure that Surewin B.V understands the nature of its customers' activities and can identify unusual or potentially suspicious behaviour, in line with regulatory requirements.

10.5 Identification and Verification of the player

Identification and verification of the player

Verification of an identity refers to actions taken to verify that a person exists and is who he claims to be. This is done by checking reliable, independent (of the person whose identity is being verified) sources.

Customers must provide sufficient, clear, and eligible documents for identification verification. The following documents are required: Evidence of identity must include a customer's full name, residential address, and date of birth as they appear in the registration account. Upon reaching the 2000 EUR threshold in deposits the information listed may be verified by obtaining one or more of the below:

- A valid unexpired passport;
- A valid unexpired national or other government-issued identity card;
- A valid unexpired residence card; or
- A valid unexpired driving license.

The verification of the residential address shall be carried out by referring to any one of the following documents:

- A recent statement from a recognised credit institution. Bank Statements are allowed only if they are issued by a subject person carrying out relevant financial business in Curacao or equivalent activities in a reputable jurisdiction.
- A recent utility bill or a similar document should be provided, ensuring that it pertains to services connected to the specific residential property.
- A rental agreement
- A correspondence from a central or local government authority, department or agency.
- Any valid unexpired government-issued document (Passport, National Identity, Driving License), where a clear indication of residential address is provided.
- Documents, other than official government issued documents, must not be more than six months old.

Documents provided to verify an address should not refer to PO Boxes or 'care of' addresses.

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.

Customers are contacted by email to their registered email address requesting them to send the documents. All documents are uploaded in electronic format using the secured platform. Received documents are inspected and compared to images of official documents of the same type. Additional information is requested if any documents do not appear to be authentic or are inconsistent with other known information about the customer.

10.6 On-Going Monitoring

Ongoing monitoring of identity

Ongoing monitoring comprises of continuous and periodic checks to ensure customers remain acceptable, identify changes that could affect a customer risk assessment and any unusual activity. This monitoring is undertaken in three parts:

- Review of CDD/EDD to ensure the information held remains accurate, up to date and appropriate for the customer relationship;
- Scrutiny of transactions to ensure they are in line with CDD/EDD and expected activity of the customer; and
- Sanctions monitoring.

Monitoring CDD/EDD

By monitoring CDD/EDD Surewin B.V can:

- Consider risk assessments for the customer and the business;
- Determine what is expected activity for the customer;
- Help protect Surewin B.V from criminals.

High risk customers will be subject to annual review of EDD including SOW.

Surewin B.V Risk Team will review CDD and EDD accordingly.

When a high risk customer is approved for play their account will be subject to a diary alert that will prompt the risk team to undertake a review of the EDD held. This prompt, delivered via email, will be sent one month before the anniversary of the account approval (and annual thereafter).

The review will consist of:

- Checking the ID document on file remains current
- Review SOW information to ensure it remains accurate using the information held on file via open source checks
- Screen for negative press via internet searches

If any of this information cannot be confirmed as current / accurate the customer will be contacted to provide updated information / documentation.

Upon review of a high risk customers EDD, the risk team will send the review via email for review and approval to a Senior Manager. Any changes to circumstances will be communicated to the MLRO for review, risk assessment and additional approval.

Standard and Medium risk customers CDD will be reviewed during a trigger event.

Valid Due Diligence

Surewin B.V takes steps to maintain valid due diligence documentation for all players. When due diligence documentation is obtained, the expiry date of the identity document is recorded. When the expiry date is approaching, a notification is sent to the Risk team who will in turn contact the player to request an updated identity document be provided.

In respect of other due diligence, such as documents provided for proof of address or source of wealth, these will be considered at trigger events and updates requested on a case-by-case basis. As a standard, if a document was provided more than two years ago updated documentation will be requested.

Should the requested documents not be provided, the case will be referred to the MLRO to consider the appropriate next steps, which may include open-source research to determine if the information held remains current or if non-traditional means can be applied.

Ongoing monitoring of transactions

In line with our risk based approach Surewin B.V must apply appropriate scrutiny to all transactions.

To achieve this the following transaction monitoring is undertaken:

- Special attention will be given to monitoring account activity, and to the extent possible, the purpose and background of any more complex or large transactions and any transactions which are particularly similar, by their nature, to be related to any form of money laundering or the funding of terrorism.
- The risk staff will be responsible for this monitoring and will review any activity that the monitoring system detects and also will determine whether any additional steps are required,
- When the risk agent detects any activity that may be unusual, he or she must notify the MLRO. The MLRO will make an in-depth decision whether or not and how to further investigate the matter.
- The organization will not accept cash or non-electronic payments from clients. Funds may be received from clients only by any of the following methods: credit cards, debit cards, electronic transfer and any other method approved by the respective regulators.
- The organization will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.
- Transfers of funds between clients' accounts are prohibited.
- To the extent the organization utilizes a third party to process and record payments to and from client and accounts, the organization will ensure the services provider has transaction monitoring systems in place which will allow for screening of the transactions to these provisions and in accordance with the applicable legislation.
- Records relating to the financial transactions shall be maintained in accordance with the data protection act.
- Fraud / Risk Management teams will monitor transactions.
- The monitoring will always be considered in line with the customer's risk assessment and

expected activity.

- Attempt to remove a card from an account or withdraw to an account which is not the same as the depositing source;
- Customer deposits for the first time with a payment method exposed to chargebacks;
- Customer tries to deposit using a credit or debit card issued in a country that does not reflect the residence of the customer;
- Customer deposits with a new payment method while having a balance in the account.

Moreover, even before reaching the two thousand Euro (€2,000) threshold, Surewin B.V has systems in place which allow it to apply a level of on-going monitoring. Through these systems, Surewin B.V ensures:

- a) To determine the moment in time when the two thousand Euro (€2,000) threshold is met.
- b) To stop players from deliberately avoiding CDD checks by staying under the €2,000 transaction limit.

The latter is ensured through the following procedures:

- a. We are able to determine the moment in time when the two thousand Euro (€2,000) threshold is met through daily reports hitting our risk inbox with a list of Customers meeting this criterion.
- b. Customers opening multiple accounts are closed to avoid having customers opening multiple to bypass the (€ 2,000) rule.
- c. We can detect the application for the opening of an account by a person who has inputted manifestly false details via our SIFT tool. Our Risk team also reviews the list of accounts opened daily to safeguard against this risk.

In such instance, when the two thousand Euro (€2,000) threshold has not been reached, there will be no need for additional CDD documentation to be collected. However, if Surewin B.V already notices inconsistencies at this stage between the information provided by the customer and any other information Surewin B.V may acquire through interaction with the customer, Surewin B.V shall question these discrepancies and take any remedial action it deems necessary, including, where applicable, filing an UTR with the FIU.

This CDD threshold is to be continuously monitored and any customers meeting the threshold should be included on the AML monitoring list.

Sift Tool

We can detect the application for the opening of an account by a person who has inputted manifestly false details. We have a tool called Sift that assists with identifying fictitious accounts.

Sift is a machine learning technology that has become the market leader in fraud prevention, acquiring customers across industries such as e-commerce, fintech, and iGaming.

Key features of Sift Technology:

- Device ID features
- Features that track email address characteristics
- Features that capture physical address characteristics

Sift has been implemented at registration for Surewin B.V

- All new accounts will be screened across Sift database for detecting promo abuse, fictitious accounts.

- Fraudsters will create multiple accounts very quickly to illegally obtain new player bonuses.
- They might change email address, change phone number, or mask their IP address.
- They will be targeting multiple operators in one go and will not have the time or the ability to change every identity signal that Sift is analysing. For example, if they change
- All signals mentioned above, Sift will be tracking the device fingerprint of the user and can link users together as such inconsistencies at this stage between the information provided by the customer and any other information Surewin B.V may acquire through the interaction with the customer, Surewin B.V shall question these discrepancies and take any remedial action it deems necessary.
- Any missed accounts will be picked up upon KYC verifications.

10.7 Timing of CDD Measures

CDD measures are to be applied when carrying out transactions amounting to two thousand Euro (€2,000) or more. The moment in time when the CDD obligations (along with carrying out a customer risk assessment) are triggered and must be applied are to be determined as follows:

In the case of an occasional transaction, the obligation to carry out CDD will be dependent on the value of the said transaction reaching or exceeding two thousand Euro (€2,000). This also applies in the case where a series of linked transactions are executed which, though individually are below the said threshold, they would cumulatively meet or exceed the two thousand Euro (€2,000) threshold. Transactions are considered as linked if they are carried out by the same customer through the same game or in one gaming session. The two thousand Euro (€2,000) is to be calculated only based on deposits made by the customer without taking into consideration any bonuses or winnings accumulated onto the account.

The two thousand Euro (€2,000) deposit threshold is calculated considering all deposits effected by a customer since the establishment of the business relationship.

Surewin B.V decided to follow the latter.

If the threshold is met, then a customer risk assessment needs to be carried out, whereby Surewin B.V is to identify the customer, verify his/her identity and, if deemed high risk, determine the customers source of wealth and the source of the funds used for the said transactions or carry out such other measures as may be sufficient to mitigate the risks identified.

The following table sets out the levels of CDD and EDD, depending on Customer Risk Assessment or trigger event.

EDD	Certified CDD			✓
	Selfie with ID – case by case basis			✓
	3rd party background – case by case basis			✓
	Open source research			✓
	SOW			✓
CDD	Evidence of Identity at threshold		✓	✓
	Transaction monitoring from initial deposit (ongoing)	✓	✓	✓
	PEP, Sanctions and Negative Press / Adverse Media screening from first deposit (ongoing)	✓	✓	✓
	Country and IP screening upon registration	✓	✓	✓
	Risk rating	Standard	Medium	High/ Unusual activity

10.8 Enhanced Due Diligence

Enhanced due diligence (EDD) is the term used to describe measures that are required to be carried out for higher risk customers in addition to the CDD requirements required for standard risk customers. Due diligence should be risk-based therefore conducting enhanced measures in higher risk scenarios will focus AML/CFT measures on the customers that pose the highest risks.

In addition to collecting EDD for higher risk customers, EDD would also be applied in the event of the following:

Unusual activity

- The customer was identified as holding a prominent position within an international organisation;
- The customer is/was involved in professional sports; or
- The customer uses multiple sources to fund their gambling activity;
- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- 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;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;

- Conducting enhanced monitoring of the business relationship;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Any request for EDD must be completed within **30 days**. If a request is not satisfied within **30 days**, the MLRO must be informed and consideration given if a UTR is required in line with the reporting procedures.

In instances of unusual activity, EDD would not be applied if it would result in tipping off a customer that there was an investigation underway.

EDD Measures

Any player that is categorised as high risk must be subject to EDD.

EDD comprises of five elements in addition to standard CDD. Four of those five elements require "consideration" as each high risk customer must be treated on a case-by-case basis - risk factors reviewed, understood, and appropriate measures taken to address the risk posed by the customer.

The four elements to consider are as follows:

1 - Additional identification information (consider if)

Obtaining additional identification information would be appropriate where risks relate to the possibility of stolen or fake identity. It can also assist in confirming or discounting potential PEP, sanctions or negative press matches or when conducting open source research.

Examples of additional information include:

- Middle names
- Aliases
- Former names
- Nationality(ies)
- Gender
- Official person identification number
- Occupation
- Name of employer
- Previous address

2 - Additional verification (consider if)

Consideration should be given to carrying out additional measures to verify the customer's identification information as part of standard CDD and to verifying additional information provided as part of the EDD.

Examples of additional verification methods include:

Obtaining additional ID documents such as driver's licence, student card or bus pass

- A telephone or video call with the customer
- Request a selfie of the customer holding their ID or outside their home address (which can then be verified using google maps, etc.)
- Verify information supplied using internet searches and open source databases (e.g. Facebook, LinkedIn)

3 - Background research (consider if)

For high risk customers, particularly those with large or unusual transactions or where there are concerns over the SOW, Surewin B.V must make efforts to establish whether the customer has been accused or convicted of proceeds generating crime (e.g. theft, fraud).

This is achieved using open source information, name screening for negative press or by commissioning third party reports.

The MLRO is experienced in undertaking such research and will assist with any such circumstances.

4 - Additional ongoing monitoring (consider how)

The policy requires all ongoing monitoring to be risk-based, therefore monitoring of high risk customer should be conducted more frequently and comprise of more extensive checks.

The type of monitoring will depend on the relevant risk factors.

As a standard the following EDD measures are applied:

- Obtaining additional ID documents such as driver's licence, student card or bus pass that has not been used a standard proof of identity
- A video call with the customer
- Obtaining a selfie of the customer holding their ID or outside their home address (which can then be verified using google maps, etc.)
- Sending a document for signature by courier to the home address for it to be signed and returned by the customer with the journey being tracked
- Verify information supplied using internet searches and open source databases or social media (e.g. Facebook, LinkedIn)

EDD will be considered on a case by case basis. In some circumstances the MLRO may advise that additional measures be applied depending on the risk factors identified.

EDD must also be conducted in the case of any suspicious activity is identified – the MLRO will advise on what EDD is required in these circumstances.

A customer will have **30 days** from the initial request to provide EDD. Should EDD not be provided within that time frame, the customer's account will be immediately suspended and consideration given to the completion of a UTR.

5 - Source of Wealth

The fifth element of EDD is source of wealth. Unlike the other elements detailed above, SOW **must** be undertaken when EDD is triggered (high risk, PEP etc).

In these circumstances, the policy sets out that Surewin B.V must reasonably establish and understand a customer's SOW.

SOW is distinct from source of funds and describes the origins of a person's financial standing or total net worth, i.e. what activities have generated the customer's funds.

The measures used to establish SOW will vary depending on the risks associated with the customer and the value of their transactions. When determining the appropriate measures the following factors will be considered:

- What factors resulted in the customer being classified as high risk;
- The value of the customer's transactions; and
- The period over which the transactions occurred and, if over a short period of time, consider what the value would be at that rate over the course of a year

Depending on the risk factors SOW will be considered using information available within the public domain, making use of social media such as LinkedIn and employee profiles on company websites. Such research will in all cases be undertaken and all considerations documented.

Surewin B.V is not required to contact a customer to establish SOW however, in this example, it would be appropriate to do so. In instances where information isn't available to source independently the following may be requested, on a case by case basis, as advised by the MLRO:

- An up to date CV
- A copy of recent bank statements
- Copies of pay slips and/or employment contract
- Details of any businesses owned
- Documentation to evidence inheritance or the sale of an asset

From the additional information provided further checks will be carried out in order to evidence if the SOW can now be verified.

In all instances, whether through independent checks or information provided by the customer, consideration will be given to:

- How reliable or independent the source of the information is;
- How plausible the information is; and
- How this compares to the customer's activity.

Source of Wealth vs Affordability

The majority of customers enjoy gambling as a leisurely activity making use of disposable income, however Surewin B.V recognises that gambling of significant portions of income should prompt interaction with the customer from a responsible gambling point of view.

Should SOW checks indicate that, when considered in line with betting activity, affordability is in question Surewin B.V will contact the customer in line with the responsible gambling policy.

Background research

During SOW verification, any information that raises any concerns or for high risk customers with large or unusual transactions Surewin B.V will conduct background research in order to establish, as far as possible, whether the customer has been accused or convicted of any crime that could have generated illicit funds such as fraud or theft.

Background research will be conducted by the Risk team who has been sufficiently trained to undertake this research.

The research will comprise of:

- Open source checks
- Name screening for negative press via screening tools
- Screening of any entity or person that forms part of their SOW

All research will be documented within the back office including any determinations made.

10.9 Simplified Due Diligence

Simplified Due Diligence (SDD) may be applied in low-risk situations where the likelihood of money laundering or terrorist financing is minimal and where permitted.

- The customer is resident in a jurisdiction with effective AML/CFT controls, not listed as high-risk by FATF or the EU.
- The product or account limits exposure to risk, e.g. low deposit limits, non-reloadable, no third-party payments, or strict withdrawal controls.
- There is no reason to suspect the customer is involved in money laundering or terrorist financing.
- The customer is not a politically exposed person (PEP).
- The customer relationship is non-anonymous, and there is no use of privacy-enhancing technologies that obscure identity (e.g., certain cryptocurrencies or VPN masking).
- Surewin B.V uses alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.).

10.10 Politically Exposed Persons

PEP's and Sanctions

Introduction

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

Screening for PEPs and Sanctions

Upon first deposit customers are screened against PEP and Sanctions lists via Namescan (and thereafter ongoing screening throughout the duration of the customer relationship).

How to Perform a PEP & Sanction search on the Namescan Screening Tool

Step 1: Log In

- ✓ Go to the [Namescan website](#)
- ✓ Log in using your authorized username and password

Step 2: Navigate to the Search Section

- ✓ Once logged in, go to the Dashboard
- ✓ Click on "New Scan"

Step 3: Enter Search Details

- ✓ In the search form, enter the full name of the individual or entity
- ✓ Optional fields (if available):
 - ✓ Date of Birth
 - ✓ Country

Step 4: Start the Scan

- ✓ Click "Search" or "Submit" to initiate the scan
- ✓ Wait for the scan to complete—usually just a few seconds

Step 5: Review the Results

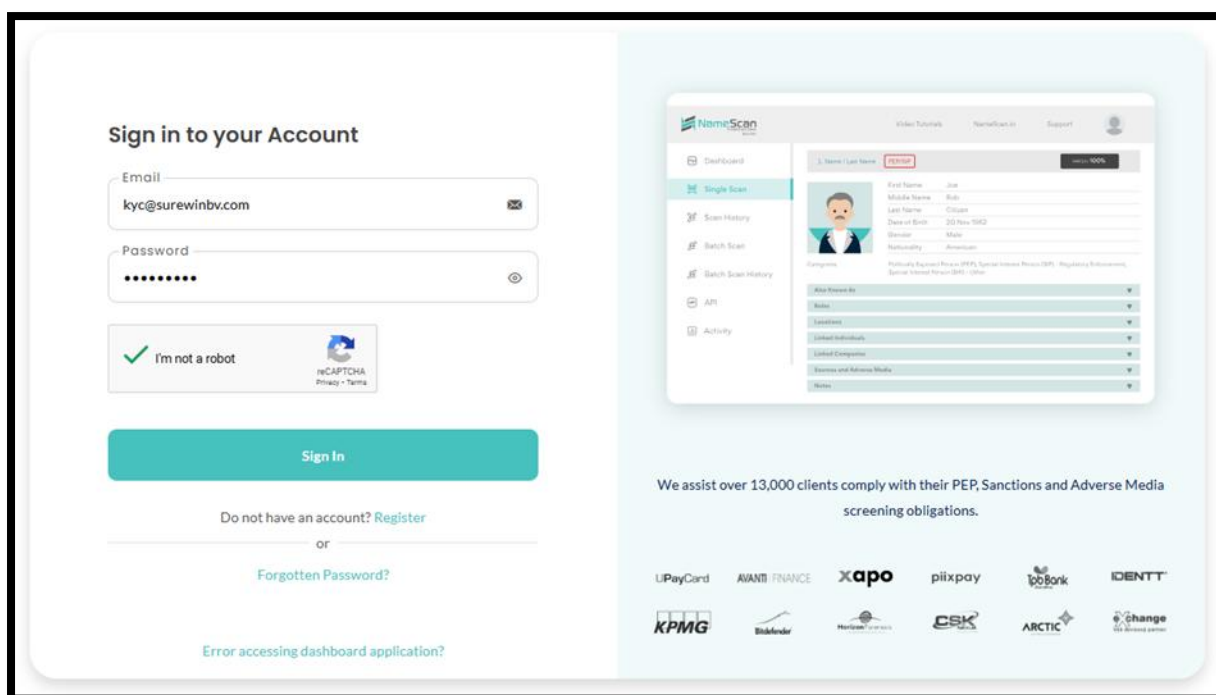
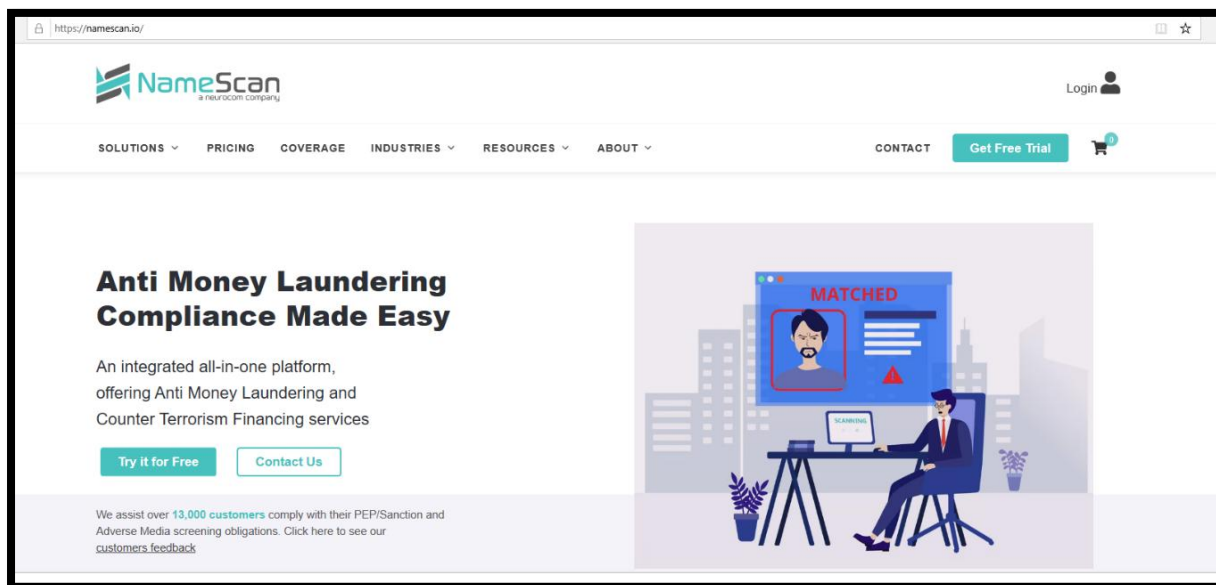
- ✓ Results will be categorized by relevance and risk level
- ✓ Review any matches carefully:
 - ✓ False Positives: No action needed
 - ✓ Potential Matches: Flag for further review or escalate to compliance

Step 6: Save or Export Results

- ✓ Save the report within the Back Office as a PDF - Ensure the report is linked to the account record for audit purposes.
- ✓ Account>KYC>Others>Choose file>
 - New Verification Status: vrfn_verified
 - Expiry: 31 - 12 - 9999
 - Document Id: NAMESCAN
 - Contact: select
- ✓ Make a note on the Back Office - NAMESCAN DONE AGAINST PEP AND SANCTIONS - NO MATCH - CERTIFICATE UPLOADED

Step 7: Update the PEP Tracker

Screenshots of the Namescan Screening Platform



The screenshot shows the 'Person' tab selected in the top navigation bar. The 'Source' section has 'Emerald' selected. The 'Scan Settings' bar at the top right shows 'List Type: All', 'Sanction List: ALL', 'FATF Jurisdiction Risk: On', 'Adverse Media: On (Google, Bing)', and 'Match Rate: > 25'. The form fields are as follows:

Field	Value
Name	Original Script (Non-Latin/Roman based languages, such as Cyrillic, Arabic, Hebrew, Chinese, etc.) is acceptable. Please provide either 'First Name and Last Name' or 'Name' in the fields provided.
First Name	ROBERT
Middle Name	GABRIEL
Last Name	MUGABE
Date of Birth	21/02/1924
Country	Zimbabwe
Gender	Male
Email Address	
Record Due Diligence Decisions	☐
Reference Number	

Buttons at the bottom right: Scan, Clear.

The screenshot shows the 'Identities' tab for a program named 'ZIMBABWE'. It displays a profile for '3) Robert Mugabe' with a 'PEP' tag. The profile includes a photo and the following details:

Field	Value
Name	Robert Mugabe
First Name	Robert
Last Name	Mugabe
Gender	male
Deceased	Yes
Deceased Date	2019-09-06
Date of Birth	1924-02-21
Place of Birth	Kutama, Zimbabwe
Update At	2023-01-16

Below the profile, there are sections for 'Reference' (Consolidated PEP List), 'Father' (Gabriel Mugabe Matibori), 'Mother' (Amai Bona Mugabe), 'Spouse' (Grace Mugabe), 'Children' (Bona Mugabe, Michael Nhamodzenyika Mugabe, Chatsungu Bellamine Mugabe, Robert Peter Mugabe Jr.), 'Sibling' (Sabina Mugabe), 'Citizenship' (Zimbabwe), and 'Occupations' (politician). There are also expandable sections for 'Other Names', 'Political Parties', 'Roles', and 'Other Information'.

Surewin B.V recognises the increased risk in dealing with PEP's and their associates. In addition, Surewin B.V recognises the prohibition on dealing with sanctioned individuals and companies.

Politically Exposed Person (PEP) are entrusted with prominent public functions or are family members or close associates of such persons. These are people in power and could be susceptible to corruption.

Surewin B.V has a process by which all High-Risk customers are checked and screened against a PEPs/Sanctions database.

PEP and Sanctions checks consists of screening customers against Namescan to determine if they are known fraudsters, drug dealers, terrorists, money launderers or politically exposed persons.

The names of customers that match the names of known fraudsters, drug dealers, terrorists or money launderers are investigated by the Risk department and any accounts that are determined or suspected to be related or owned by a known fraudster, drug dealer, terrorist or money launderers

are escalated to the MLRO for review.

Surewin B.V through the application of risk variables, Surewin B.V will be able to mitigate the risks posed by the threat of being used for money laundering and/or terrorist financing.

Customers should not be able to log in, play, or request any deposits or withdrawals during the time the account is under review.

- **Where a potential PEP match can be discounted** as a false positive, details of the investigation and rationale for discounting must be recorded within the back office on the player profile and recorded on the discounted PEP log.
- The discounted PEP log is reviewed on a monthly basis by the Compliance Officer.
- **Where a potential PEP match cannot be discounted** as a false positive **or where the match is confirmed as positive PEP** must be subject to EDD including SOW.
- Upon receipt of EDD a PEP Assessment must be completed.
- Only when EDD including SOW and a successful PEP Assessment is completed can the approval of the relationship be considered
You leave the following note on the account:
 - Risk Management review complete. False positive from Namescan. (If all other checks are completed, no other fraud has occurred, and senior management has cleared the customer the account can be reopened).

PEP Risk Assessment

Upon identification of a PEP the level of risk that they pose must be assessed. In order to do so meaningfully the following factors will be taken into account:

- The level of influence that the individual holds;
- The scale of their public profile;
- The level of seniority within their organisation or Government;
- Authority over or access to state funds and assets, policies and operations;
- Control over regulatory approvals, awarding of licences and concessions.

Surewin B.V will complete a PEP Risk Assessment in each instance – the assessment template is included in this manual at Schedule 3. This is completed by the Risk team and sent to the Directors and/or The MLRO for review. All PEP relationships must be approved by the Directors and/or The MLRO.

10.10.1 Ongoing Monitoring of PEP Screening

Should a player who had not been identified as a PEP at on-boarding stage become one, Surewin B.V will implement measures described above within the thirty-day window of observing that the person is a PEP. Failing with these, shall result in Surewin B.V terminating the relationship with this customer.

10.10.2 Sanctions Match

Surewin B.V must ensure it does not transact with any person who is subject to sanctions. Specific actions taken regarding customers identified on sanctions lists:

- A record of customers on sanctions lists identified and reported is kept by the Compliance team.
- Any match will result in the customer's account being immediately frozen and details sent to the MLRO and Directors of Surewin B.V

Surewin B.V must ensure it does not transact with any person who is subject to sanctions. In order to monitor this all customers are screened against current sanctions upon deposit via Namescan and thereafter ongoing screening throughout the duration of the customer relationship against relevant sanctions lists.

10.11 Application of CDD measures to existing customers

Surewin B.V applies ongoing Customer Due Diligence (CDD) measures to existing customers in accordance with AML/CTF regulations. This ensures that customer information remains accurate, relevant, and up to date throughout the relationship lifecycle.

10.11.1 Risk-Based Review

- Customers are categorized by risk level (standard, medium, high), and CDD reviews are conducted accordingly.
- Review frequency:
 - **High-risk:** Annually
 - **Medium-risk:** Every 2–3 years
 - **Standard-risk:** Every 3–5 years

10.11.2. Trigger Events - CDD is reapplied if:

- There is a change in customer information
- Unusual or suspicious transactions occur.
- Regulatory or legal updates apply (e.g., sanctions).

10.11.3. Ongoing Monitoring

Customer activity is monitored continuously by Risk staff and at trigger events to detect deviations from expected behaviour. Any anomalies may prompt enhanced due diligence (EDD).

10.11.4. CDD Measures

For existing customers, the following must be reviewed and updated as needed:

- Identity and verification documents
- Business purpose and transaction patterns
- Source of funds or wealth (where applicable)
- Screening against sanctions and adverse media

10.11.5. Roles and Responsibilities

All customer-facing teams, Compliance Officers, and operations staff are responsible for ensuring timely CDD updates. Escalation procedures apply for high-risk or non-cooperative customers.

10.11.6. Recordkeeping

CDD documentation will be retained for at ten years.

10.12 The termination of the business

A customer might not be willing to provide Surewin B.V with the necessary information or documentation even though Surewin B.V may have repeatedly solicited him/her to forward said information or documentation. In this case, in addition to keeping a record of all the attempts made, the following needs to be followed:

- a) If the requested information and documentation is not received within **30 days** from the moment the threshold/trigger event was reached. Surewin B.V will terminate its business relationship with the customer, i.e., it is not to allow service to the customer. To this end, Surewin B.V may decide to either close the account or to keep it blocked and suspended in its entirety. In the latter case, we ensure that the account has a NIL balance at the time it is blocked and suspended, with any funds standing to the credit of any such account being disposed of as set out hereunder. If the customer makes the requested information and/or documentation available to Surewin B.V following the closure or the suspension and blocking of the gaming account, Surewin B.V will consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given customer.
- b) Surewin B.V considers whether there are any grounds giving rise to suspicion of ML/FT. The reluctance of the customer to provide CDD documentation on its own should not be automatically equated to a suspicion of ML/FT. Surewin B.V also considers all factors and information it has at its disposal, including for example the payment method used, the played, and the customers playing trends and patterns, any information on the customer already held, including his/her jurisdiction of residence, and information which can be obtained through sources such as the internet etc. If there are grounds to suspect ML/FT, then the team will submit an Unusual Transaction Report (“UTR”) to the FIU. Should there be grounds to suspect ML/FT, then the MLRO is informed promptly, and an UTR is to be filed at the earliest possible even though the thirty days allowed for the collection of the necessary CDD information or documentation may not have lapsed or the customer may not have approached Surewin B.V to carry out any further transactions.
- c) Where there are no grounds to suspect ML/FT or the transaction has not been suspended by the FIU or by operation of the law, nor is there an attachment or freezing order, Surewin B.V would have no reason rooted in the AML/CFT regime justifying the retention of any such funds.
- d) Thus, where funds are to be remitted back, Surewin B.V should:
 - Consider whether there is any other legal impediment to the remittance of the funds; and
 - Remit the funds to the same source through the same channels used to receive the funds.

If Surewin B.V is unable to remit the funds to the same source through the same channels, it will inevitably have to request fresh instructions from the customer. If these instructions give rise to suspicion, this should be raised with the MLRO as a potential UTR and suspend the remittance pending the FIU expressing its opposition or otherwise to the said transaction.

Whenever funds are remitted, it is also, to the extent that this may be possible, indicate in script/instructions accompanying the funds that these are being remitted due to the customers' inability to complete CDD.

10.13 Reliance on third parties to perform customer due diligence

- The third party must be regulated, supervised, or monitored for AML compliance in a jurisdiction with equivalent standards.
- The third party must retain all relevant documents and information for at least 10 years.
- Surewin B.V remains ultimately responsible for the adequacy and accuracy of the CDD performed.
- Surewin B.V will monitor the performance and reliability of the third party.
- Periodic audits or reviews may be conducted to ensure ongoing compliance with CDD requirements.

Recordkeeping and Documentation

- A record of all reliance arrangements must be maintained, including:
 - Identity of the third party
 - Jurisdiction and regulatory status
 - Date and scope of reliance
 - Access logs to CDD documentation

11. Reporting of unusual Transactions

11.1 Introduction

Surewin B.V has established the following procedures and controls to ensure.

- All officers, management and staff know that any unusual activity should be reported to the MLRO.
- Such reports can be easily and clearly reported to the MLRO.
- The MLRO has full access to any information that may be of assistance to consider such a report and decide on whether the activity is usual.
- That any necessary external disclosure to the FIU can be made by the MLRO as soon as possible.
- All UTRs, external disclosures and ML/FT/PF enquiries are properly recorded.

The following transactions or intended transactions are deemed unusual:

- a) Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b) Transactions in the amount of two thousand five hundred Euros (€2,500) or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:
 1. A cashless transaction in the amount of two thousand five hundred Euros (€2,500) or

more.

2. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
3. Accepting or releasing a deposit in the amount of two thousand five hundred Euros (€2,500) or more at the request of the client;
4. Sale to a customer of chips in the amount of two thousand five hundred Euros (€2,500) or more. "Chips" include but is not limited to tokens and credits.
5. A cash out in the amount of two thousand five hundred Euros (€2,500) or more;

Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent to two thousand five hundred Euros (€2,500) or more and is considered per gaming day.

- d) Presumed money laundering transactions or terrorist financing: transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

11.2 Recognition of Unusual Transactions

During the course of ongoing monitoring activity or registration unusual activity may be identified that does not fit the expected pattern of activity. When this occurs, further scrutiny is required to determine if the unusual activity is unusual.

Unusual activity is any activity, including the receipt of information, where:

- Transactions are:
 - Overly complex;
 - Both large and unusual;
 - Of an unusual pattern;
- There is no apparent economic or lawful purpose;
- We doubt the identity of a customer;
- We doubt any aspect of the information we hold about a customer.

When unusual activity is identified the customer's account will be disabled and an immediate investigation undertaken. This will comprise of:

- Conducting EDD; and
- Conducting appropriate scrutiny of the activity in question -
 - Investigate until the activity to obtain sufficient
 - Consider using a broad range of data sources – e.g. open source/ search engines, social networks etc.
 - Review the customer's historic activity to detect any patterns
 - Consider the CDD/EDD on file

Unusual activity is any activity, including the receipt of information, which causes us to:

- Know or suspect; or
- Have reasonable grounds to know or suspect that the activity or information is related to ML, FT or PF.

When unusual activity is identified the customer's account will be disabled and a UTR must be made to the MLRO using the UTR form included at Schedule 2.

It is important to note that EDD would not be applied if this would tip off the customer that their account was under investigation.

11.3 Reporting Unusual Transactions

- If, after appropriate scrutiny, you have reasonable grounds for knowledge or suspicion of ML/FT/PF a report must be made to MLRO immediately.
- All suspicions should be reported to the MLRO using the "UTR" form, this can be made available to you by the MLRO via email. A copy is also attached as Schedule 2. The UTR must be completed in full of as much information included as possible in order for the MLRO to understand and consider your suspicions. Copies of any relevant EDD and transactional activity should be included.
- It is vital that you do not discuss your report with anyone else as you may commit the offence of tipping off.
- Failure to report could result in serious consequences.
- Upon receipt of your disclosure the MLRO will issue you with an acknowledgement of receipt of the report. You should keep this receipt in a safe place as it is documentary evidence that you have complied with the requirement to report any suspicions you may have. Do not place the receipt on any shared file, or any other file that can be accessed by other staff members. This is to ensure that no one else is aware that you have made a report of unusual activity.
- You are obliged to continue to submit reports of any further suspicions you might have.

What happens after a report is made?

The MLRO will assess the information contained within the report, together with any other relevant information, to determine whether there are reasonable grounds for knowing or suspecting that the activity is related to ML/FT or PF.

If the MLRO considers that there are reasonable grounds for knowing or suspecting that the activity is related to ML/FT or PF they must make an external disclosure to the FIU as soon as practicable.

To demonstrate the conclusions reached in relation to each UTR, the MLRO must retain records which show the assessment of the report, and the decision reached. These records are kept in the UTR register which is confidential to the MLRO.

Following receipt of a UTR or any external disclosure that does not result in the customer relationship being exited, considerations will have made on any impact to the customer risk assessment. Any change in risk classification will be communicated by the MLRO.

There are red flags that may alert Surewin B.V, but they are merely indicative and need not necessarily be taken on their own point to ML/FT taking place. See list below:

- Customers do not cooperate in the carrying out of CDD.
- Customer attempts to register more than one account with Surewin B.V
- Customer deposits considerable amounts during a single session by means of multiple pre-paid cards.
- Customer deposit funds well more than is required to sustain usual betting patterns.

- Customers make small wages, 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 enquiries about the possibility of moving funds between accounts belonging to the same gaming.
- 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 unusual behaviour in playing games that are considered as high risk.
- IP linked to other player accounts.
- Use of multiple deposit methods in a short span of time.
- Large deposits and minimal activity.
- Address Verification Failure.
- Deposit of funds not followed by wagering.
- Adverse media.
- Attempt to use payment sources belonging to a third party.

11.4 AML/CFT Registers

The MLRO maintains separate registers to evidence compliance with the UTR requirements and to provide useful information to identify trends that can be used for training purposes and risk assessment.

The registers are kept up to date at all times and entries are recorded as soon as a disclosure is made/received with further detail added as the matter progresses.

Access to the registers is restricted to the MLRO, Compliance Officer and the Directors to ensure the sensitive information recorded within them remains restricted.

There are three registers:

- UTRs - any type of UTR made to the MLRO.
- External disclosures - ML/FT/PF/Sanctions disclosures made to the FIU or intelligence disclosures made under Section 24 of the FIU Act; and
- Enquiries received by competent authorities

The MLRO must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU.

12. Record Keeping

Surewin B.V will only enter a business relationship with a customer in circumstances where the customer has opened an account with us. There can be no occasional or one-off transactions. Surewin B.V. keeps the following records in relation to all customers: transaction documents, due diligence information, and information relating to unusual transactions. These documents will be retained as set out in the AML Procedure and in accordance with the Data Retention Policy:

- transaction documents
- CDD information
- information relating to unusual transactions.

The Data Protection Officer and the compliance team manage and retain the data listed above in accordance with the applicable data protection laws and regulations.

12.1 Retention Periods

The length of time that records are retained depends on what that record is. The retention periods applied are as follows:

Record Type	Retention Period
Transaction records (as described above)	10 years from the date of completion of the transaction
AML/CFT records	10 years beginning on the date the customer relationship was formally ended, or if not formally ended, when all activity was completed.

In the case of any records that relate to an external disclosure being made or that is subject to any investigation by a competent authority, Surewin B.V must maintain all relevant records for as long as required by the competent authority. Guidance in this period can be sought from the relevant authority in these instances.

It is important to note that the above retention periods continue to apply should Surewin B.V cease to operate.

13. No Cash Policy

No cash deposits / withdrawals will be affected. Surewin B.V does not accept any cash transactions.

14. Employee screening program and ongoing employee training program

Surewin B.V will carry out a thorough interview with any potential staff member prior to making an offer of employment. In advance of the interview process, the candidate will be required to present their CV which will be analysed prior to and during the interview process. Should an offer of employment be made, the necessary steps will be taken to substantiate the information and documentation received during the interview.

14.1 Employee Screening Process

Following any offer of employment all proposed new employees will be vetted. The process applied to vet staff consists of, wherever possible:

- Obtain CDD;
- Obtain and confirm references;
- Confirm employment history;
- Confirm any qualifications advised;
- Request details of any regulatory action taken against the individual;
- Request details of any criminal convictions;
- Screening for negative press.

The above will be requested for all staff. In cases where the above cannot be provided for non-key staff, the Directors reserve the discretion to waive the requirement if justifiable. An example being in the event of being unable to obtain a reference for a junior member of staff who lacks any employment history.

Any appointment to a senior position a criminal records check will be undertaken. This check will further bolster the above information and confirmation of a satisfactory check will be provided to the Curacao GCB should the Boards approval be required for a key person position.

If an existing member of staff is promoted to a senior position, they too will be subject to a police check.

Surewin B. V's Human Resources department will be responsible for updating the Human Resources file to include the supporting documentation outlined above and issuing an offer of employment and Employment Contract.

A register of all staff members is maintained within the Human Resources files.

14.2 Security Function

Surewin B.V will maintain a Security function to detect potential internal fraud. This function will also serve the purpose of highlighting errors by operators and will provide feedback to the business on a regular and timely basis.

The Operations department will monitor activity of a manual nature that is carried out by the Surewin B.V staff on customer accounts, e.g., manual settlements, manual adjustments. If the team concludes there has been fraudulent activity, they will notify the management and if required this will be reported to the police.

The team submits weekly reports to various Heads and Managers that highlight any errors made by staff. Any discrepancies will be escalated to the Finance Manager as soon as the error is identified to reclaim any funds and to notify the line manager.

14.3 System Controls

Surewin B.V will also implement a series of systems controls, designed to prevent individuals from unilaterally adjusting details of customer accounts or having unnecessary access to back-office systems.

The Service Desk/IT Department will continue to manage access permissions that staff have within

various teams as per Service Desk/IT processes. Notwithstanding the monitoring activity of the operations team, customer-facing departments will continue to operate a 'sign-off' system for manual adjustments that ensures a more senior person signs off on the adjustment being made.

14.4 Training

Surewin B.V will provide relevant employees with a programme of training in relation to the topics and themes considered by this Policy and the Procedure. Enhanced training will also be provided to relevant staff members on a regular basis, specifically in relation to obligations under both legislative and licensing requirements. Further training may also be offered, as needed, when policies and procedures are reviewed and amended from time to time. A written record will be retained of all training received by employees in accordance with this AML Policy.

Enhanced training programmes e.g. obligations under legislative and licensing requirements, will be delivered on a regular basis to relevant staff, including when regulation and licensing requirements change, and whenever the AML policy, this procedure is documented, and relevant processes change.

Surewin B. V's AML training shall be appropriately tailored to Surewin B. V's activities and shall indicate the different levels of Money Laundering risks and vulnerabilities associated with Surewin B. V's business activities. Surewin B.V is obliged to take appropriate and proportionate measures from time to time to:

- (a) Ensure that the employees are aware of the relevant AML Regulations and data protection requirements as well as of Surewin B. V's AML measures, policies, controls and procedures; and
- (b) Provide training in relation to the recognition and handling of operations and transactions, if applicable, that may be related to proceeds of criminal activity, money laundering or financing of terrorism.
- (c) A written record of staff attendance/participation, and certifications attained where applicable, are retained centrally.

15. External Data Requests

The AML & CFT Policy and Procedure will set out the process by which Surewin B.V B.V. will respond to lawful enquiries from third parties who are seeking to obtain information in relation to Surewin B.V customers. Surewin B.V will seek to respond to all such enquiries promptly, with a view to cooperating with lawful requests to the fullest extent reasonably possible.

On occasions, Surewin B.V receives enquiries from third parties seeking to obtain information /data in relation to Surewin B.V customers.

The Compliance team will, as soon as practicable, evaluate and manage every AML request in accordance with relevant data protection regulations, internal data protection policies, and in accordance with AML codes of practice, license conditions, and guidance published and or issued by the relevant authorities.

The Compliance team will respond promptly to all AML requests, and will fully co-operate reasonably possible, as per internal data protection policies and procedures.

16. Third Party Relationships

Surewin B.V conducts a risk-based programme of due diligence in relation to third parties with whom we conduct business.

The Compliance team are responsible for conducting due diligence checks on all third-party suppliers, on a risk-based basis. Any negative findings will be referred to the Management and the MLRO as appropriate.

17. Audit Function

Surewin B.V Anti-Money Laundering (AML) compliance program will undergo an independent audit at least once a year. The audit will evaluate key areas, including:

- AML, Counter-Terrorist Financing (CTF), and Counter-Financing of Proliferation (CFP) manuals
- Customer file reviews
- Compliance management processes
- Transaction testing
- Adequacy of employee training
- Adherence to relevant laws and regulations
- System capability to detect unusual activity
- Interviews with frontline transaction staff and supervisors
- Sampling and review of transactions above reporting thresholds
- Record retention practices

18. Breach of this Policy

Employees must ensure that they read, understand and comply in full of the letter and spirit of this policy. Any employee who fails to do so may face disciplinary action.

Schedule 1 - Glossary

Acronym	Detail
AML	Anti-Money Laundering
ML/FT	Money Laundering and Financing Terrorism.
CDD	Customer Due Diligence
CTF	Counter- Terrorist Financing
EDD	Enhanced Due Diligence
UTR	Unusual Transaction Report
KYC	Know Your Customer
PEP	Politically Exposed Person
WMD	Weapons Mass Destruction
DDO	Due Diligence Obligation
NOIS	National Ordinance on Identification of Clients when rendering Services
NORUT	National Ordinance on the Reporting of Unusual Transaction
FIU	The Financial Intelligence Unit
SOW	Source of Wealth
UTR	Unusual Transaction Report
SDD	Simplified Due Diligence
CAP	Customer Acceptance Policy
AML/CFT	Anti-Money Laundering/Counter Financing of Terrorist
PF	Proliferation Finance
TRA	Technical Risk Assessment
BRA	Business Risk Assessment
CRA	Customer Risk Assessment
IBAN	International Bank Account Number
BIC	Bank Identifier Code
HNWI	High Net Worth Individuals
ID	Identity Document
RNG	Random Generator Number
PDF	Portal Document Format
MLRO	Money Laundering Officer

Schedule 2 - Unusual Transaction Report (UTR) Template

Unusual Transaction Report (UTR) Template Document with guidance notes

Internal Unusual Transaction Report		
1	Team:	e.g., CDD/Customer Services
2	Time and Date:	HH:MM:DD Mon YY
3	Customer Details:	Account number User ID Name Date of Birth Address Email Telephone
4	Linked Accounts:	Account Numbers, details of relationship i.e., linked via device, linked via IP, family member, same household etc.
5	Customer:	VIP etc. if applicable
6	Account Status:	Active/Suspended/Closed

7	Account Balance & Pending Withdrawals:	Note: All pending withdrawals should be held pending AML review
8	Grounds for suspicion:	Include as much detail as possible, outlining all relevant factors and reasons that criminality is suspected, i.e., fraudulent payment methods, links to criminal activity or persons, spend out of gauge with customer profile, open source information or unusual transactions on site
9	Miscellaneous Info:	

Schedule 3 – PEP Assessment Form

PEP Assessment Form

Notes:

- This form MUST be completed when potential PEP Status is indicated for any customer
- No account activity can be undertaken until a PEP relationship has senior sign off

Date of this assessment/review:	
Name of person under assessment/review:	
Customer ID	

Search findings

Background information leading to the PEP classification:	
PEP status (per the AML/CFT Policy):	PEP PEP (family member) PEP (close associate)
Screening findings (attach copy obtained for this review):	PEP status confirmed / Not confirmed
Sanctions list checks (attach copy of report obtained for this review):	Findings / No Findings
Google (attach copy of search results)	Findings / No findings
Details of any other research or information obtained which indicates or evidences PEP status:	
EDD	Confirm what EDD has been sourced (attach copies)
Proof of identity	
Proof of residential address	
SOW	
Other	
Any betting activity (if a change in status since registration)	
Country of residence	
Any other observations or concerns?	

Director / MLRO Recommendation

PEP relationship approved?	Yes	No
Recommended steps to monitor risk:		
Any further EDD required? If yes, list	Yes	No

Schedule 4 - Sanctions Assessment Form

Sanctions Assessment Form

Notes

- This form **MUST** be completed when potential Sanctions Status is indicated for any customer
- Where a potential match is identified, additional information and EDD will be obtained in order for the validity of that potential match to be considered.
- No account activity can be undertaken until a relationship has senior sign off

Date of this assessment/review	
Name of person under assessment/review	
Customer ID	

Search findings

Date of Potential Match	
Name of subject	
Type - Individual or Entity	
Regime	
Listed Date	
Details of possible connection	
Staff member who identified possible connection	
False positive?	
Details of curing	
Further action	
Sanctions list checks (attach copy of report obtained for this review): Findings / No Findings	
Google (attach copy of search results) Findings / No Findings	
Details of any other research or information obtained which indicates or evidence Sanction Status	
EDD	Confirm what EDD has been sourced (attach copies)
Proof of identity	
Proof of residential address	
SOW	
Other	
Any betting activity	

(if a change in status since registration)	
Country of residence	
Any other observations or concerns?	

Director / MLRO Recommendation

Sanctions approved?	Yes	No
Recommended steps to monitor risk:		
Any further EDD required? If yes, list	Yes	No
Director / MLRO name, signature and date		
*Return to customer service team		

Customer Service Team - Action points

Update sanction register 'Added to Sanctions Register' date	Next review date: *diary for annual review	
Confirm ongoing monitoring in place	Yes	No
Signed by person preparing form	(name)	
Date	(date)	