



Surewin B.V

AML/CFT POLICY



VERSION 2

CONTENTS

KEY INFORMATION.....	6
1. POLICY STATEMENT	6
2. PURPOSE	7
3. AUDIENCE.....	7
4. DEFINITIONS	8
4.1 WHAT IS MONEY LAUNDERING	8
4.2 STAGES OF MONEY LAUNDERING.....	8
4.3 THE PURPOSE OF THESE STAGES:.....	8
4.4 HOW WE MIGHT BE ABUSED BY MONEY LAUNDERERS	9
4.5 WHAT IS THE FINANCING OF TERRORISM?.....	9
4.6 WHAT IS THE FINANCING OF PROLIFERATION OF WEAPONS?	10
4.7 WHAT IS TARGETED FINANCIAL SANCTION?.....	10
4.8 POLICY IMPLEMENTATION.....	12
5. GOVERNANCE AND OVERSIGHT.....	12
5.1 BOARD OF DIRECTORS	12
5.2 SENIOR MANAGEMENT.....	13
5.3 MONEY LAUNDERING REPORTING OFFICER (MLRO)	13
5.4 COMPLIANCE DEPARTMENT	13
5.5 RISK DEPARTMENT	13
5.6 CUSTOMER DUE DILIGENCE (CDD).....	14
5.7 TRANSACTION MONITORING AND REPORTING.....	14
5.8 SANCTIONS AND PEP SCREENING.....	14
5.9 ACCOUNT BLOCKING PROCEDURE (FOR ML/TF SUSPICION)	14
5.10 TRAINING AND AWARENESS	14
5.11 RECORDKEEPING	14
6. BUSINESS RISK ASSESSMENT (BRA)	15
6.1 GEOGRAPHICAL RISK	15
6.2 JURISDICTIONAL RISK FACTORS	15

6.3 CUSTOMER RISK	16
6.4 TRANSACTION RISK	16
6.5 PRODUCT RISK	18
6.6 DISTRIBUTION CHANNELS RISK	18
6.7 EMPLOYEE RISK	19
6.8 CUSTOMER RISK ASSESSMENT	19
7. CUSTOMER RISK MATRIX	22
7.1 CUSTOMER ACCEPTANCE POLICY	23
7.2 UNACCEPTABLE CLIENTS	25
8. CUSTOMER DUE DILIGENCE	26
8.1 CUSTOMER DUE DILIGENCE (CDD) MEASURES	27
8.2 IDENTIFICATION AND VERIFICATION OF THE BENEFICIAL OWNER	28
8.3 BENEFICIAL OWNERSHIP VERIFICATION	28
8.4 IDENTIFICATION AND VERIFICATION — LEGAL ENTITIES	29
8.5 BENEFICIAL OWNER IDENTIFICATION — THRESHOLD AND METHODOLOGY	30
8.6 COMPLEX OWNERSHIP STRUCTURES	30
8.7 SPECIFIC STRUCTURE TYPES	30
8.8 WHEN BENEFICIAL OWNERSHIP CANNOT BE ESTABLISHED	30
8.9 ONGOING MONITORING OF LEGAL ENTITY CUSTOMERS	31
9. OBTAINING INFORMATION ON THE PURPOSE AND INTENDED NATURE OF THE BUSINESS RELATIONSHIP ... 31	
9.1 IDENTIFICATION AND VERIFICATION OF THE CUSTOMER	32
9.2 ONGOING MONITORING	34
9.3 SIFT TOOL	38
9.4 ENHANCED DUE DILIGENCE	40
9.4.1 <i>Unusual activity</i>	40
9.4.2 <i>EDD Measures</i>	40
9.4.3 <i>Source of Funds and Source of Wealth</i>	42
10. SIMPLIFIED DUE DILIGENCE	48
11. PEP'S AND SANCTIONS	48

11.1 PEPS (POLITICALLY EXPOSED PERSON)	48
11.2 SCREENING FOR PEPS AND SANCTIONS	48
11.3 PEP RISK ASSESSMENT	53
11.4 ONGOING MONITORING OF PEP SCREENING.....	54
11.5 SANCTIONS MATCH	54
12. APPLICATION OF CDD MEASURES TO EXISTING CUSTOMERS.....	54
12.1 ONGOING MONITORING.....	55
12.2 ROLES AND RESPONSIBILITIES.....	55
12.3 RECORDKEEPING	55
12.4 THE TERMINATION OF THE BUSINESS RELATIONSHIP.....	55
12.5 RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE.....	56
13. REPORTING OF UNUSUAL TRANSACTIONS.....	57
13.1 RECOGNITION OF UNUSUAL TRANSACTIONS	59
13.2 REPORTING UNUSUAL TRANSACTIONS.....	60
13.4 REPORTING TIMEFRAMES AND ESCALATION RESPONSIBILITIES	60
<i>Escalation Responsibilities</i>	62
<i>Tipping-Off Prohibition</i>	62
14. RECORD KEEPING	63
14.1 MINIMUM RETENTION PERIOD	63
14.2 FORMAT AND ACCESSIBILITY	64
15. OBJECTIVE AND SUBJECTIVE INDICATORS	65
16. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM.....	66
17. EMPLOYEE SCREENING PROGRAM AND ONGOING EMPLOYEE TRAINING PROGRAM	70
18. SECURITY FUNCTION.....	71
19. SYSTEM CONTROLS	71
20. TRAINING.....	72
21. AML/CFT AUDIT AND ASSURANCE FRAMEWORK.....	72
21.1 RISK-BASED AUDIT PLANNING.....	73
21.2 MINIMUM AUDIT SCOPE	74
21.3 AUDIT METHODOLOGY.....	75

21.4 AUDIT RATING	75
21.5 REMEDIATION	76
21.6 AUDIT REPORTING	76
21.7 BOARD OVERSIGHT	77
21.8 CONTINUOUS ASSURANCE	77
21.9 AUDIT RECORDS	77
22. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE	78

Document Version Control

Version	Date	Person Responsible	Changes Partial/New
1	18 November 2025	Craig Murugan	New
2	17 June 2026	Craig Murugan	Partial

KEY INFORMATION

Approving Official(s):

Senior administrator(s) responsible for approving the policy.

Responsible Office:

Office responsible for policy dissemination, updates, and reviews.

Effective Date:

Month, day, and year the policy (or revision) takes effect.

Next Review Date:

1. POLICY STATEMENT

Surewin B.V is firmly committed to the highest standards of integrity and transparency in all its operations. Recognizing the critical role that the Curaçao Gaming Authority (CGA) plays in regulating and safeguarding the gaming industry, we fully adhere to Curaçao's AML/CFT legal framework, including the Landsverordening Identificatie bij Dienstverlening (LID), Landsverordening Melden Ongebruikelijke Transacties (LMOT), and the CGA AML/CFT Regulations effective January 2025.

The Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) framework is established to safeguard the integrity of the financial system and to ensure compliance with both national and international obligations. This framework is grounded in the legal authority provided by the Sanctions National Ordinance (N.G. 2014, no. 55) and the Kingdom Sanction Act (N.G. 2016, no. 54). These legislative instruments empower competent authorities to impose, enforce, and monitor sanctions, thereby strengthening the jurisdiction's resilience against illicit financial flows and the financing of terrorism. These legislative frameworks establish the foundation for compliance with national and international sanctions regimes and inform the sanctions screening, monitoring, and risk management controls outlined throughout this policy.

This policy establishes a comprehensive and risk-based approach to preventing and mitigating risks associated with money laundering and terrorist financing within our online gaming operations. It outlines the internal controls, governance structures, and operational procedures that ensure early detection, timely reporting, and effective management of suspicious activities in accordance with CGA standards.

Through ongoing training, rigorous customer due diligence, continuous transaction monitoring, and a culture of compliance, Surewin B.V strives to contribute to the integrity of the Curaçao gaming jurisdiction and uphold its reputation as a responsible and law-abiding gaming operator.

Scope - To prevent the customers from exploiting the company for purposes of money laundering and terrorist financing, the company is fully committed to complying with the laws and regulations of its licensing bodies and all the applicable FATF recommendations. The purpose of this document 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 the company.

2. PURPOSE

Surewin B.V is fully committed to preventing any activity related to money laundering and terrorist financing within its gaming operations. We maintain a robust Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) program that complies with all applicable Curaçao laws, including the LID, LMOT, and the Curaçao Gaming Authority's AML/CFT regulations.

Our commitment extends to:

- Implementing effective customer due diligence and ongoing monitoring measures.
- Ensuring all unusual transactions are promptly reported to the Financial Intelligence Unit (FIU).
- Providing continuous AML/CFT training for all employees and management.
- Cooperating fully with regulatory authorities and law enforcement.
- Conducting regular internal audits and reviews of our AML/CFT controls.

Through these efforts, Surewin B.V seeks to protect the integrity of the Curaçao gaming sector, prevent illicit financial activity, and uphold the trust of our customers and stakeholders.

3. AUDIENCE

This Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) policy applies to all individuals and entities involved in or associated with Surewin B.V operations, including but not limited to:

- **All employees**, across all departments and levels of seniority.
- **Management and Board members**, responsible for governance and oversight.
- **Subcontractors and consultants** engaged to perform functions related to gaming operations or compliance.
- **Third-party suppliers and service providers**, including payment processors, software vendors, and customer verification services.
- **Affiliates** acting on behalf of the company.

All stakeholders are expected to understand, comply with, and support the implementation of this policy in accordance with their roles and responsibilities. This Policy should be followed always, and non-compliance will be treated in an extremely serious manner. If at any time it is impractical to follow the provisions of the Policy, written permission to deviate from the

procedures must be obtained from the board of directors of Surewin B.V and the MLRO, before any action is taken.

4. DEFINITIONS

4.1 WHAT IS MONEY LAUNDERING

AML is the acronym for anti-money laundering. Money Laundering is an 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 money.

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

4.2 STAGES OF MONEY LAUNDERING

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.

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

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.

4.3 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?"

4.4 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 customer's account.
- Layering – Small amounts are used to gamble.
- Realization – The balance of the account is withdrawn showing the origin being a legitimate source successfully disconnecting themselves from the original property.

4.5 WHAT IS THE 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.

4.6 WHAT IS THE FINANCING OF PROLIFERATION OF WEAPONS?

Proliferation of weapons of mass destruction ("WMD") can be in many forms but ultimately involves the transfer or 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.

4.7 WHAT IS TARGETED FINANCIAL SANCTION?

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 organization or element within them.

Sanctions are generally imposed on:

- 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, stigmatizing 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 Curacao and to all Curacao people (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 registration 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 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.

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 customer so an account cannot be registered in the future.

LID (Landsverordening Identificatie bij Dienstverlening): The National Ordinance on the Identification of Service Providers, requiring customer identification and verification as a prerequisite to providing services.

LMOT (Landsverordening Melding Ongebruikelijke Transacties): The National Ordinance on the Reporting of Unusual Transactions, requiring certain service providers to report unusual or suspicious activity to the FIU.

CGA (Curaçao Gaming Authority): The licensing and supervisory body responsible for enforcing AML/CFT compliance standards among licensed gaming operators in Curaçao.

FIU Curaçao (Financial Intelligence Unit): The designated government agency that receives, analyzes, and disseminates reports on unusual or suspicious financial transactions.

PEP (Politically Exposed Person): An individual who holds, or has held, a prominent public function (e.g., government officials, senior executives of state-owned enterprises), as well as their immediate family members and close associates. PEPs are subject to Enhanced Due Diligence.

Customer Due Diligence (CDD): The process of identifying, verifying, and assessing customers to understand the risk they pose.

Enhanced Due Diligence (EDD): Additional verification applied to higher-risk customers, such as Politically Exposed Persons (PEPs) or those from high-risk countries.

Beneficial Owner: The natural person(s) who ultimately owns or controls a legal entity or account.

Unusual Transaction: A transaction that deviates from a customer's normal or expected activity and may indicate suspicious behavior.

Sanctioned Person or Entity: Any individual or organization listed on national or international sanctions lists, with whom business dealings are prohibited or restricted.

Risk-Based Approach (RBA): A method of allocating AML/CFT resources and controls proportional to the risk level identified.

4.8 POLICY IMPLEMENTATION

This section outlines how the Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) policy will be operationalized. It identifies the responsible stakeholders, defines their roles, and references associated procedures and oversight mechanisms.

5. GOVERNANCE AND OVERSIGHT

5.1 BOARD OF DIRECTORS

- Holds ultimate accountability for AML/CFT compliance.
- Is responsible for approving this AML/CFT Policy, any material amendments to it, the Business Risk Assessment, and the overall AML/CFT compliance framework of Surewin B.V.
- All Board and senior management decisions relating to AML/CFT governance, including policy approvals, approval of material amendments, review of the Business Risk Assessment, review of annual MLRO reports, approval of risk appetite changes, and review of significant AML/CFT incidents or remediation actions, will be formally documented in Board or committee minutes.

Surewin B.V will maintain an AML Governance Log recording, at minimum:

- the date of each Board or committee AML/CFT discussion or approval;
- the document or matter considered;
- the decision taken;
- the persons in attendance;
- any action items arising;
- the responsible owner for each action; and
- the target completion date and closure status.

Board minutes, governance logs, policy approval records, annual MLRO reports, Business Risk Assessment approval records, audit reports and remediation records will be retained for a

minimum of five (5) years and made available to the Curaçao Gaming Authority or any competent authority upon request.

5.2 SENIOR MANAGEMENT

- Ensure implementation of the AML/CFT program, allocation of resources, and coordination among departments.
- Supports a culture of compliance throughout the organization.

5.3 MONEY LAUNDERING REPORTING OFFICER (MLRO)

- Appointed to manage the day-to-day AML/CFT compliance framework, including investigations, risk monitoring, and unusual activity reporting. Acts as the main point of contact for the FIU Curaçao and CGA.

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 regulatory or legislative amendments are reflected. Any amendments are approved by the Directors and MLRO.

5.4 COMPLIANCE DEPARTMENT

- Maintains and updates procedures, conducts training, performs internal audits, and ensures ongoing adherence to legal obligations.
- Oversees third-party vendors where applicable.

5.5 RISK DEPARTMENT

- Risk Assessment & Mitigation. Classify customers and transactions by risk levels (low, medium, high)
- Support onboarding by reviewing documents for identity verification, age checks, and source of funds.
- Transaction Monitoring & Fraud Detection.
- Reporting & Escalation

5.6 CUSTOMER DUE DILIGENCE (CDD)

- Performed before entering a business relationship, at the latest when a customer reaches the threshold of NAf 4,000 (€2,000) in cumulative deposits or transactions.
- CDD includes identity verification, beneficial ownership checks, and risk classification.
- Enhanced Due Diligence (EDD) is applied to high-risk customers such as PEPs or users from high-risk jurisdictions.
- Responsible Department: Risk Department

5.7 TRANSACTION MONITORING AND REPORTING

- Transactions are continuously monitored for unusual patterns or red flags.
- Any transaction exceeding NAf 5,000 (€2,500) or appearing suspicious must be escalated to the MLRO.
- The MLRO files Unusual Transaction Reports (UTRs) with the FIU Curaçao in accordance with LMOT.
- Responsible Department: MLRO / Risk Department

5.8 SANCTIONS AND PEP SCREENING

- All customers and counterparties are screened against international and local sanctions lists (UN, EU, OFAC) and PEP databases during onboarding and regularly thereafter.
- If a customer is flagged as a match, their account is reviewed and escalated to the MLRO for decision-making.
- Responsible Department: MLRO / Risk Department

5.9 ACCOUNT BLOCKING PROCEDURE (FOR ML/TF SUSPICION)

- When activity is flagged as suspicious, the MLRO conducts a rapid review.
- Accounts may be temporarily blocked to prevent further transactions.
- If suspicion is confirmed, the MLRO will file an UTR and determine next steps, including potential account closure.
- Responsible Department: MLRO / Compliance Team

5.10 TRAINING AND AWARENESS

- All employees receive AML/CFT training at onboarding and annually.
- Enhanced training is delivered to customer-facing and compliance staff.
- Training records are maintained for regulatory inspections.
- Responsible Department: Compliance Team / Training Manager

5.11 RECORDKEEPING

- CDD records, transaction logs, UTR filings, and risk assessments are retained for at least 10 years.
- Secure digital storage ensures accessibility and confidentiality.
- Responsible Department: Compliance Team / IT

6. BUSINESS RISK ASSESSMENT (BRA)

- Conducted at least annually or upon material changes (e.g., new markets, products, or regulations).
- Identifies and mitigates ML/TF risk across products, customer segments, and jurisdictions.
- Informs updates to the AML program and controls.
- Responsible Department: Compliance Team / MLRO / Risk Committee
- 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 conducting 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 customer or prospective customer. 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").

6.2 JURISDICTIONAL RISK FACTORS

Customers 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 making 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 organizations operating within them.
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

6.3 CUSTOMER RISK

It is critical to determine the potential money laundering and/or terrorist financing risks posed by our customers 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 customer 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 customers.

Surewin B.V needs to be aware of its customers overall spending by monitoring their activity and transactions as this information is important to determine whether the customers 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 customers on its database. Customers are categorized in 3 main categories: Standard Risk, Medium Risk, and High Risk.

6.4 TRANSACTION RISK

Changes to financial institution accounts

Customers 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 customer's account i.e., 5 cards are allowed where a customer 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 payouts with how the customer deposited to carry out gambling transactions. Hence, where it is feasible, funds will be returned to customers 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 customer 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 customer'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 customer's account. These copies must display the customer's signature together with the first six and last four digits of the card itself. For the customer's own security and safety, customers should block out the security number at the back and the middle digits on the front of their card.
- Wallets - A screenshot of your wallet account showing the customer's email address/account number and personal account information.
- Bank Statement - A bank statement issued in the last 3 months for the customer's bank account. This should include the customer'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 - Customers 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.
- Customers using vouchers are assigned a high-risk score. Should a customer use pre-paid vouchers and less risk deposit methods, the customer is nonetheless assigned a higher risk, irrespective of the frequency and amount deposited through prepaid vouchers.
- Inter account transfers - Transferring funds from one customer to another customer is strictly prohibited. This is also stated in our Terms and Conditions, which customers 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 customer accounts to carry out ML.

6.5 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.

6.6 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 customers are asked to fill in a detailed registration form, so that they can be duly identified.
- Customers' Identities are verified on a risk-sensitive basis.

6.7 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.

6.8 CUSTOMER RISK ASSESSMENT

Surewin B.V carries out a CRA at the establishment of a business relationship, including when a player registers an account or reaches the transaction threshold (e.g., cumulative deposits exceeding NAf 4,000 / €2,000) and that the risk assessment must estimate the risk of ML/FT/PF posed by the customer. The assessment must be recorded and regularly reviewed to ensure it remains up to date.

The assessment informs the customer's risk profile, which determines the level of due diligence, frequency of monitoring, and ongoing review requirements.

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

Any customer 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 customer 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 customer that is a PEP.
- a customer that is HNWI.
- persons performing prominent functions for international organizations.
- customers that are sporting professionals betting on sports.
- customers 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 customer 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 customer 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.

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 customer's 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.

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 participants 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 participants' 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 participants 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 customer 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.

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 whether 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.

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.

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. CUSTOMER 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 customer 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 customer	Deposit below 4,000 NAf (Below €2,000 Euro)
Medium (A customer must meet two of the criteria to be considered medium risk)	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 customer	Cumulative Deposit or withdrawal between NAf 4,000 – NAf 20,000 (between approx. €2,000 - €10,000 Euro)

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 customer	Cumulative Deposit or withdrawal above 20,000 NAf (Above €10,000 Euro)
PROHIBITED	Business participants	Closed / blocked jurisdictions	Cash or payment facility not attributable to customer	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 participant's 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 analyzed by the Surewin B.V Risk team.

Surewin B.V Risk Team provides the following services in relation to customers 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.

7.1 CUSTOMER ACCEPTANCE POLICY

The Customer Acceptance Policy ("CAP") sets out the principles and criteria that Surewin B.V applies when deciding whether to open, maintain, restrict or terminate a customer relationship. It forms part of Surewin B. V's AML/CFT framework and is intended to ensure that

the business only accepts customers whose risks can be properly identified, assessed, monitored and managed.

The purpose of the CAP is to:

- protect Surewin B.V from exposure to money laundering, terrorist financing, proliferation financing, sanctions and fraud risks;
- prevent the business from being used, knowingly or unknowingly, for unlawful or suspicious activity;
- identify customers who may present a higher level of risk and ensure that appropriate due diligence and monitoring measures are applied;
- set out when a customer may be accepted, when enhanced controls are required, and when a relationship must be refused or ended; and
- ensure that all customer relationships remain within Surewin B. V's approved risk appetite and AML/CFT control framework.

Customer Risk Assessment at Onboarding

- Before a customer is accepted, Surewin B.V will carry out customer due diligence and assess the level of risk presented by that customer. This assessment will consider all relevant information available at onboarding, including:
- the customer's identity and verification status;
- the customer's age, location and eligibility to use the services;
- jurisdictional and geographic risk;
- payment method risk and any source of funds indicators;
- expected account activity and purpose of the relationship;
- PEP, sanctions and adverse media screening results; and
- any other risk indicators identified through the company's Business Risk Assessment, Customer Risk Assessment or internal controls.
- Each customer will be assigned a risk classification in line with the company's customer risk methodology. This risk rating will determine the level of due diligence, approval, monitoring and review that will apply to the relationship.

Higher-Risk Customers

- A higher-risk customer is not automatically prohibited from using Surewin B. V's services. However, where a customer is assessed as high risk, the relationship may only proceed if the identified risks can be properly managed through enhanced controls.
- Depending on the nature of the risk, Surewin B.V may apply one or more of the following measures:
- enhanced due diligence and additional verification checks;
- source of funds and, where appropriate, source of wealth enquiries;
- increased monitoring of deposits, withdrawals, gameplay and account activity;

- escalation to the MLRO, Compliance Officer or senior management for review and approval; and
- more frequent ongoing reviews of the customer relationship.

Refusal, Restriction and Termination of Relationships

- Surewin B.V will refuse to establish, or may restrict, suspend or terminate, a customer relationship where:
- the customer fails or refuses to provide information or documentation required for customer due diligence, enhanced due diligence or ongoing monitoring;
- the customer's identity cannot be satisfactorily verified;
- false, misleading, altered or suspicious information or documents are provided;
- the customer is subject to sanctions or other legal or regulatory restrictions;
- the customer is suspected of money laundering, terrorist financing, proliferation financing, fraud or other criminal activity;
- the source of funds, source of wealth or account activity cannot be reasonably explained where such information is required;
- the customer attempts to bypass, frustrate or manipulate the company's AML/CFT controls, verification requirements or account restrictions; or
- the overall risk presented by the customer falls outside Surewin B. V's risk appetite and cannot be adequately mitigated.

Ongoing Customer Acceptance

Customer acceptance is not a once-off decision. Surewin B.V will continue to review customer relationships throughout their lifecycle and may reclassify, restrict, suspend or terminate a customer where new information, behavioural patterns, transaction activity, screening results or other risk indicators give rise to concern or change the customer's risk profile.

All decisions to accept, reject, escalate, restrict or terminate a customer relationship must be recorded in line with the company's recordkeeping and approval procedures.

7.2 UNACCEPTABLE CLIENTS

Surewin B.V will not establish or continue a business relationship with any customer whose profile presents an unacceptable AML/CFT, sanctions, fraud or legal risk. The categories below are examples of customers that Surewin B.V will not accept. This list is not exhaustive, and the company may refuse or terminate any relationship where the overall risk cannot be appropriately managed within its AML/CFT framework.

Customers who will be considered unacceptable include:

- customers who fail or refuse to provide the information or documents required to complete customer due diligence, enhanced due diligence or ongoing monitoring;
- customers whose identity cannot be satisfactorily verified, or where the information provided appears false, inconsistent, altered or unreliable;

- customers who are subject to sanctions, asset freezing measures or other legal restrictions;
- customers who are acting on behalf of sanctioned persons or entities, or who appear to be attempting to evade sanctions controls;
- customers where there are reasonable grounds to suspect money laundering, terrorist financing, proliferation financing, fraud or other criminal activity;
- customers whose funds are known or reasonably suspected to derive from illegal or illicit activity;
- customers who attempt to bypass or frustrate the company's due diligence, verification or monitoring processes;
- customers involved in illegal business activities or activities that create an unacceptable AML/CFT risk, including serious criminal conduct, trafficking, counterfeit goods, exploitation-related offences, prohibited weapons or proliferation-related activity; and
- customers whose risk profile falls outside the company's approved risk appetite and cannot be adequately managed through enhanced due diligence or other controls.

Politically Exposed Persons and Other Higher-Risk Customers

A customer's status as a Politically Exposed Person ("PEP"), family member or close associate does not automatically make that customer unacceptable. However, such customers must be subject to enhanced due diligence, appropriate approval and enhanced ongoing monitoring in line with this Policy.

Sanctions Screening and Escalation

All customers and counterparties will be screened against relevant sanctions lists and screening databases in accordance with the company's sanctions procedures. Any potential or confirmed sanctions match must be escalated immediately to the MLRO and handled in line with internal procedures and applicable legal obligations.

Where a customer falls within an unacceptable category, or where the company reasonably believes that the customer presents an unacceptable risk, the matter must be escalated to the MLRO and/or Compliance for review. The decision to refuse, restrict or terminate the relationship, together with the reasons for that decision, must be properly documented.

8. CUSTOMER DUE DILIGENCE

Surewin B.V adheres to and complies with "Know Your 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.

8.1 CUSTOMER DUE DILIGENCE (CDD) MEASURES

CDD measures are not in principle applicable until the Naf 4,000 (€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 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 their bets may be forfeited, and all 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 customer, 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 four thousand Naf 4,000(€2000 Euro) 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 four thousand Naf 4,000(€2000 Euro) are nonetheless monitored and if an unusual deposit or game activity is noted, they are nonetheless subjected to KYC.

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

8.2 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 organization, their account will be immediately frozen and suspended.

8.3 BENEFICIAL OWNERSHIP VERIFICATION

Surewin B.V will apply the appropriate Customer Due Diligence (CDD) measures to identify and verify the entity, its ownership structure, and its beneficial owners. In addition, all beneficial owners will be screened against applicable UN, EU, and Kingdom of the Netherlands sanctions lists, in accordance with the Sanctions National Ordinance (N.G. 2014, no. 55) and the Kingdom Sanction Act (N.G. 2016, no. 54).

In such circumstances, Surewin B.V will:

- **Obtain and verify entity details:** Legal name, registration number, registered address, and constitutional documents.
- **Identify beneficial owners:** Any natural person who owns or controls 25% or more of the entity, directly or indirectly.
- **Verify control:** Any natural person exercising ultimate effective control through ownership, voting rights, management control, or other means.

- **Understand ownership structure:** Obtain sufficient information to map the ownership and control chain.
- **Verify authority:** Confirm authority of persons acting on behalf of the entity.
- **Apply Enhanced Due Diligence:** For complex, opaque, unusual, or high-risk structures.

Surewin B.V requires identification and verification of all natural persons who ultimately own or control a legal entity, with a threshold of 25% ownership or control. For complex structures such as trusts, layered corporate ownership, or nominee shareholders, enhanced procedures apply:

For complex structures such as trusts, layered corporate ownership, or nominee shareholders, enhanced procedures apply:

- All intermediate layers of ownership must be documented and verified.
- For trusts, the settler, trustee(s), protector (if any), and beneficiaries must be identified and verified.
- For multi-jurisdictional entities, verification must include certified documentation from each jurisdiction of incorporation.
- Where beneficial ownership cannot be established with reasonable certainty, the business relationship will be refused.

Where Surewin B.V is unable to identify or verify the beneficial owner(s), or where the ownership structure cannot be reasonably understood, the business relationship will not be established or will be terminated, and the matter escalated to the MLRO for review.

8.4 IDENTIFICATION AND VERIFICATION — LEGAL ENTITIES

For any legal entity customer or counterparty, the following information must be obtained and verified before establishing or continuing a business relationship:

- Full legal name as registered.
- Registered address and principal place of business.
- Company or entity registration number and jurisdiction of incorporation.
- Constitutional documents (e.g., articles of incorporation, memorandum and articles of association, partnership agreement, trust deed).
- Names and identity of directors, authorised signatories, and persons with authority to act.
- Ownership and control structure, including a current organisational chart where available.
- Confirmation of the entity's legal status and good standing (e.g., certificate of good standing, registry extract dated within six months).

8.5 BENEFICIAL OWNER IDENTIFICATION — THRESHOLD AND METHODOLOGY

The beneficial owner(s) of a legal entity are identified as any natural person who:

- Directly or indirectly owns or controls 25% or more of the shares or voting rights; or
- Exercises ultimate effective control by other means (management rights, contractual arrangements, veto powers, rights to appoint/remove directors).

Where no natural person meets the threshold, the senior managing official(s) responsible for day-to-day management will be identified and treated as the beneficial owner for CDD purposes. This determination must be documented and approved by the MLRO.

Risk-Based Flexibility: In higher-risk scenarios (e.g., politically exposed persons, high-risk jurisdictions, complex structures), Surewin B.V may apply a lower threshold for beneficial ownership identification.

8.6 COMPLEX OWNERSHIP STRUCTURES

For entities owned or controlled through layers of companies, trusts, foundations, or nominee arrangements, Surewin B.V will:

- Map the full ownership chain to identify all intermediate and ultimate beneficial owners.
- Apply Enhanced Due Diligence to each layer presenting elevated ML/TF risk.
- Obtain a written explanation for the structure's legitimate business purpose.
- Verify the identity of each beneficial owner using documentary standards required for natural persons.
- Document the full chain of ownership in the customer's file.

8.7 SPECIFIC STRUCTURE TYPES

- **Trusts:** Identify and verify settlor(s), trustee(s), protector (if any), beneficiaries, and any person exercising ultimate control.
- **Foundations:** Identify and verify founder, council members, beneficiaries, and persons exercising effective control.
- **Nominee Shareholders/Directors:** Obtain nominee agreements, identify and verify the underlying principal, and treat the principal as the beneficial owner.

8.8 WHEN BENEFICIAL OWNERSHIP CANNOT BE ESTABLISHED

Where Surewin B.V is unable to identify or verify one or more beneficial owners:

- The business relationship will not be established; or
- If during an existing relationship, play will be suspended immediately and the MLRO notified.
- The MLRO will assess whether a UTR should be submitted to the FIU Curaçao.
- The decision and rationale must be recorded in writing and retained on file.

8.9 ONGOING MONITORING OF LEGAL ENTITY CUSTOMERS

Legal entity customers are subject to ongoing monitoring obligations, including:

- Ownership and control information reviewed at least annually or upon trigger events (e.g., director change, restructuring, adverse media).
- Any change in beneficial ownership will be reverified using onboarding standards.
- MLRO must be notified of any material change in structure, jurisdiction, or control.
- Recordkeeping: All beneficial ownership documentation will be retained for at least five years after the end of the business relationship, in line with FATF and CGA requirements.

9. 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 it is 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 sources 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.

9.1 IDENTIFICATION AND VERIFICATION OF THE CUSTOMER

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 four thousand Naf 4,000 (€2000 Euro) threshold in deposits the information listed may be verified by obtaining one or more of the following:

- 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 will be carried out by referring to any one of the following documents:

- A recent statement from a recognized 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
- Some 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 regarding 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.

Politically Exposed Persons (PEP) Screening:

Customers are screened against PEP databases. Identified PEPs are subject to Enhanced Due Diligence (EDD), including detailed source of funds investigations and frequent reviews.

Sanction-Screening:

Customers and counterparties are screened against relevant international and local sanctions lists such as those maintained by the United Nations, European Union, and OFAC. Screening is conducted at onboarding and regularly thereafter.

Freezing of Funds and Reporting:

Unusual Activity Detection: If during CDD or transaction monitoring, suspicious activities are detected (e.g., transactions involving sanctioned individuals, unusual patterns, or high-risk behavior), the funds may be temporarily frozen to prevent further movement.

Escalation and Investigation: The Money Laundering Reporting Officer (MLRO) conducts an immediate review of flagged accounts or transactions.

Reporting to Authorities: When suspicion of money laundering or terrorist financing is confirmed or cannot be ruled out, the MLRO files an Unusual Transaction Report (UTR) with the Financial Intelligence Unit (FIU) Curaçao in accordance with the Landsverordening Melden Ongebruikelijke Transacties (LMOT).

Account Actions: Depending on the findings, accounts may be suspended or closed following regulatory guidelines, and appropriate internal and external actions are taken.

9.2 ONGOING 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 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 activity is expected for the customer.
- Help protect Surewin B.V from criminals.

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

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

When a high-risk customer is approved to 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 customers. 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 customer 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 larger 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 MLRO. 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 will 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 four thousand NAf 4,000 (€2,000 Euro) 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 four thousand NAf 4,000 (€2,000 Euro) threshold is met.
- b) To stop customers from deliberately avoiding CDD checks by staying under the NAf 4,000 (€2,000 Euro) transaction limit.

The latter is ensured through the following procedures:

- a. We are able to determine the moment in time when the four thousand NAf 4,000 (€2,000 Euro) 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 four thousand NAf 4,000 (€2,000 Euro) 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 open daily to safeguard against this risk.

In such instance, when the four thousand NAf 4,000 (€2,000 Euro) 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 will 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 in the AML monitoring.

9.2.1 Linked Transactions Detection and Escalation

Surewin B.V will maintain procedures to identify linked, connected or structured transactions that, when viewed individually, may appear below applicable monitoring or due diligence thresholds, but when aggregated indicate a higher ML/TF/PF risk or an attempt to avoid AML/CFT controls.

Linked transactions may include, without limitation:

- multiple deposits, withdrawals or transfers conducted within a short period of time that cumulatively exceed a relevant threshold;
- repeated deposits followed by minimal gameplay and withdrawal activity;
- repeated use of different cards, wallets, bank accounts or payment instruments by the same customer;
- use of multiple accounts, devices, IP addresses or payment instruments indicating possible common control or coordinated activity;
- splitting transactions into smaller amounts to avoid triggering CDD, EDD, source of funds checks or internal review thresholds;
- repeated failed deposits followed by successful deposits through alternative methods;
- rapid deposit and withdrawal patterns inconsistent with the customer's known profile, source of funds or expected gambling behaviour.

Surewin B.V will aggregate relevant customer activity across accounts, payment methods, devices and time periods to determine whether transactions are linked for AML/CFT monitoring purposes.

Where linked transaction indicators are identified, the Risk Team and/or Compliance Team will:

1. record the alert and rationale in the customer file or case management system;
2. review the customer's account activity, payment instruments, gameplay behaviour, source of funds information and customer risk rating;
3. apply additional due diligence or Enhanced Due Diligence where appropriate;
4. escalate the matter to the MLRO without delay where the activity appears unusual, suspicious, structured or inconsistent with the customer profile; and
5. where appropriate, restrict, suspend or block the account pending review.

The MLRO will determine whether the activity gives rise to an obligation to submit an unusual transaction report to the FIU Curaçao and will document the decision, rationale, action taken and any follow-up measures.

9.3 SIFT TOOL

We can detect the application for the opening of an account by a person who has input 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 customer 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 analyzing. 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 will question these discrepancies and take any remedial action it deems necessary.
- Any missed accounts will be picked up upon KYC verifications.

Timing of CDD Measures

CDD measures are to be applied when carrying out transactions amounting to four thousand Naf 4,000(€2000 Euro) 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 four thousand NAF 4,000 (€2,000 Euro). This also applies in the case where a series of linked transactions are executed which, though individually are below the said threshold, cumulatively meet or exceed the four thousand NAF 4,000 (€2,000 Euro) 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 four thousand NAF 4,000 (€2,000 Euro) 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 four thousand NAF 4,000 (€2,000 Euro) deposit threshold is calculated considering all deposits affected 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 on registration (ongoing)	✓	✓	✓
	Country and IP screening upon registration	✓	✓	✓
	Risk rating	Standard	Medium	High/ Unusual activity

9.4 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:

9.4.1 UNUSUAL ACTIVITY

- The customer was identified as holding a prominent position within an international organization;
- 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 customer. Examples of sources 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 given consideration 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.

9.4.2 EDD MEASURES

Any customer that is categorized 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 being 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 license, 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 customers 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 license, student card or bus pass that has not been used as 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 MLRO may advise that additional measures be applied depending on the risk factors identified.

EDD must also be conducted in the case of any u 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.

9.4.3 SOURCE OF FUNDS AND SOURCE OF WEALTH

As part of Enhanced Due Diligence ("EDD"), the company will obtain, assess and, where appropriate, verify a customer's Source of Funds ("SOF") and Source of Wealth ("SOW").

SOF/SOW enquiries and verification must be undertaken where EDD is triggered, including where a customer is classified as high-risk, identified as a PEP, connected to a high-risk jurisdiction, subject to adverse media, or where the customer's activity, transaction pattern, payment method usage, linked transactions, deposit behaviour, withdrawal behaviour, or overall profile gives rise to concerns regarding the legitimacy of the funds used or the origin of the customer's wealth.

The company may also require SOF and/or SOW information on a risk-based basis before or after the CDD threshold is met where this is necessary to understand the customer, the source

of deposited or wagered funds, or the legitimacy of the business relationship. Surewin B.V will obtain, assess, and where appropriate verify a customer's Source of Funds (SOF) and Source of Wealth (SOW).

- Source of Funds refers to the origin of the specific funds used by a customer for deposits, gambling activity, and other transactions conducted through the Company's platform.
- Source of Wealth refers to the origin of a customer's overall wealth and how that wealth has been accumulated.

For all high-risk customers (including PEPs, customers from high-risk jurisdictions, and those with complex ownership structures), Surewin B.V requires formal verification of both Source of Funds (SOF) and Source of Wealth (SOW).

- Acceptable documentation includes bank statements, payslips, audited financial statements, proof of asset ownership, or notarized declarations.
- Verification must be completed prior to onboarding or continuation of the business relationship.
- Any inconsistencies or incomplete documentation must be escalated to the MLRO within 24 hours for review.
- The MLRO may require additional Enhanced Due Diligence (EDD) measures before approval.

SOF and SOW assessments will be undertaken where Enhanced Due Diligence measures are required, including but not limited to:

- Customers classified as high-risk;
- Politically Exposed Persons (PEPs), their family members, and close associates;
- Customers connected to high-risk jurisdictions;
- Customers subject to adverse media findings;
- High net worth individuals
- Reactivated accounts after long periods of dormancy
- Customers exhibiting unusual, complex, or potentially suspicious activity;
- Customers whose transaction activity is inconsistent with their known profile; and
- Any other circumstances where the company determines that additional due diligence is necessary to mitigate Money Laundering, Terrorist Financing, Proliferation Financing, fraud, or sanctions-related risks.

Surewin B.V will obtain sufficient information and documentation to reasonably establish the legitimacy of a customer's funds and wealth. Documentation may include, but is not limited to:

- Bank statements;
- Proof of income or employment;
- Payslips or employment contracts;
- Business ownership information and financial statements;
- Investment or dividend records;
- Inheritance documentation;

- Asset sale agreements; and
- Any other reliable evidence appropriate to the customer's risk profile.

Verification Standards

Surewin B.V will take reasonable measures to verify the Source of Funds and Source of Wealth information obtained. The extent of verification will be proportionate to the customer's risk profile and the nature, value, and frequency of transactions conducted.

For customers subject to Enhanced Due Diligence and those classified as high-risk, SOF and SOW information must be supported by independent and reliable documentation or information obtained from reputable external.

Where appropriate, information obtained will be corroborated through independent verification measures, including:

- Open-source intelligence (OSINT) research;
- Adverse media screening;
- Sanctions screening;
- PEP screening;
- Third-party verification sources; and
- Any other verification measures deemed necessary by the company.

Surewin B.V will assess whether the customer's known financial circumstances reasonably support their level of gambling activity and transactional behaviour.

Source of Wealth vs Affordability

The majority of customers enjoy gambling as a leisurely activity making use of disposable income; however, Surewin B.V recognizes 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.

Documentation and Record Keeping

All SOF and SOW assessments is documented within the company's systems and retained in accordance with applicable legal and regulatory record-keeping requirements.

The documented record includes, at a minimum:

- The reason the SOF/SOW assessment was conducted;
- Information and documentation obtained;
- Verification measures undertaken;
- Any discrepancies, concerns, or adverse findings identified;
- The risk assessment outcome;

- Any restrictions, monitoring measures, or conditions applied to the account; and
- Any approvals, decisions, or escalations to the MLRO.

Records provide a clear audit trail demonstrating the rationale for decisions taken and the measures applied in accordance with the company's risk-based CDD and EDD obligations.

Ongoing Monitoring and Review

SOF and SOW information is reviewed on an ongoing basis and reassessed where there is:

- Material changes in customer activity;
- A significant increase in deposit or wagering activity;
- A change in payment methods or funding sources;
- A change in the customer's risk classification;
- New adverse media, sanctions, or PEP information; or
- Any other information that gives rise to concerns regarding the legitimacy of funds or wealth.

High-risk customers will be subject to periodic EDD reviews, including reassessment of SOF and SOW where appropriate.

Escalation and Enhanced Measures

Where Surewin B.V is unable to reasonably establish or verify a customer's SOF or SOW, or where information provided is inconsistent, incomplete, unverifiable, or gives rise to suspicion, it will be escalated to the MLRO for review.

Surewin B.V require additional documentation, apply enhanced monitoring measures, restrict account activity, suspend transactions, terminate the business relationship, submit an unusual transaction report, or take any other action deemed necessary to mitigate identified risks.

No customer will be permitted to continue high-risk activity where the legitimacy of their Source of Funds or Source of Wealth cannot be reasonably established.

SOF/SOW Verification Standards by High-Risk Scenario

To ensure consistent and proportionate application of SOF and SOW verification across all elevated-risk categories, the following minimum standards apply. Where more than one category applies to a customer, the most stringent standard governs.

High-Risk Category	SOF Verification Required	SOW Verification Required	Minimum Acceptable Documentation
PEP (or PEP by association)	Mandatory	Mandatory	Payslips / employment letter; bank statements (3 months); declaration of public income; asset register

High-Risk Category	SOF Verification Required	SOW Verification Required	Minimum Acceptable Documentation
High Net Worth Individual (HNWI)	Mandatory	Mandatory	Audited accounts / investment statements; proof of business ownership; inheritance documentation; property valuations
High-Risk Jurisdiction	Mandatory	Strongly recommended	Bank statements (3 months); utility bills; employer confirmation; third-party income verification
Reactivated Dormant Account (inactive ≥ 12 months)	Mandatory	Where activity change detected	Updated bank statements; explanation of dormancy; re-confirmation of current employment/income status
Disproportionate Spender / Unusual Transaction Pattern	Mandatory	Mandatory if cumulative deposits exceed NAF 20,000 (€10,000) in 30 days	Payslips; tax returns; business income evidence; gift/loan declaration with third-party confirmation
Adverse Media / Criminal Allegations	Mandatory	Mandatory	MLRO-directed on a case-by-case basis; may include court documents, regulatory findings, or third-party agency reports
Multiple / Third-Party Payment Methods	Mandatory for each method	As directed by MLRO	Proof of ownership for each payment instrument; written explanation of use; account statements per method

Documentation Standards and Verification Timelines

The following standards apply to all SOF/SOW documentation regardless of scenario:

- All documentation must be obtained in its original form or as a certified copy.
- Bank statements and financial records must be dated within three (3) months of the date of request unless the MLRO specifically approves a longer period in writing.
- Where documentary evidence cannot be independently obtained, Surewin B.V may accept a signed customer declaration only when supported by at least one corroborating source (e.g. open-source financial data, LinkedIn employment records, company registry listings).
- All SOF/SOW evidence must be uploaded to the customer record within the back-office system.
- The MLRO must review and sign off on all SOW assessments for PEPs and HNWIs before the account is approved for continued play.

Verification Timelines

Timelines for SOF/SOW requests are as follows:

Scenario	Customer Response Deadline	Action if Not Received
EDD triggered at registration (PEP, HNWI, High-Risk Jurisdiction)	30 days from request	Account blocked; MLRO considers UTR submission to FIU
EDD triggered during ongoing monitoring (reactivation, pattern change)	30 days from request	Account suspended; MLRO review; relationship termination considered
Disproportionate spend / unusual transaction	30 days from request	Account must be frozen immediately; MLRO review; UTR raised if no satisfactory response
Adverse media / criminal allegation identified	As directed by MLRO (typically 7–14 days)	Account remains suspended; MLRO determines whether UTR and/or relationship termination is required

Where it is assessed that requesting SOF/SOW information would tip off the customer that an investigation is underway, the MLRO may waive the customer request requirement and instead rely solely on internal open-source verification. This determination must be recorded in writing.

Documentation Requirements

The following must be recorded in the customer's file for every SOF/SOW assessment:

- The trigger event or category that initiated the assessment;
- The date the request was issued to the customer (where applicable);
- A list of all documentation or information obtained;
- The MLRO's or Risk Team's written assessment of whether SOF/SOW has been sufficiently established;
- The outcome decision (approved, restricted, terminated) and the name of the approving officer;
- Any open-source research conducted and its results; and
- The date the assessment was completed and filed.

All SOF/SOW records must be retained for a minimum of five (5) years from the end of the business relationship or the date of the last transaction.

10. 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 customer's identity (e.g. birth certificates, bank statements etc.).

11. PEP'S AND SANCTIONS

11.1 PEPs (POLITICALLY EXPOSED PERSON)

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 refer to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

11.2 SCREENING FOR PEPs AND SANCTIONS

Customers are screened against PEP and Sanctions lists at registration 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 be complete usually just a few seconds

Step 5: Review the Results

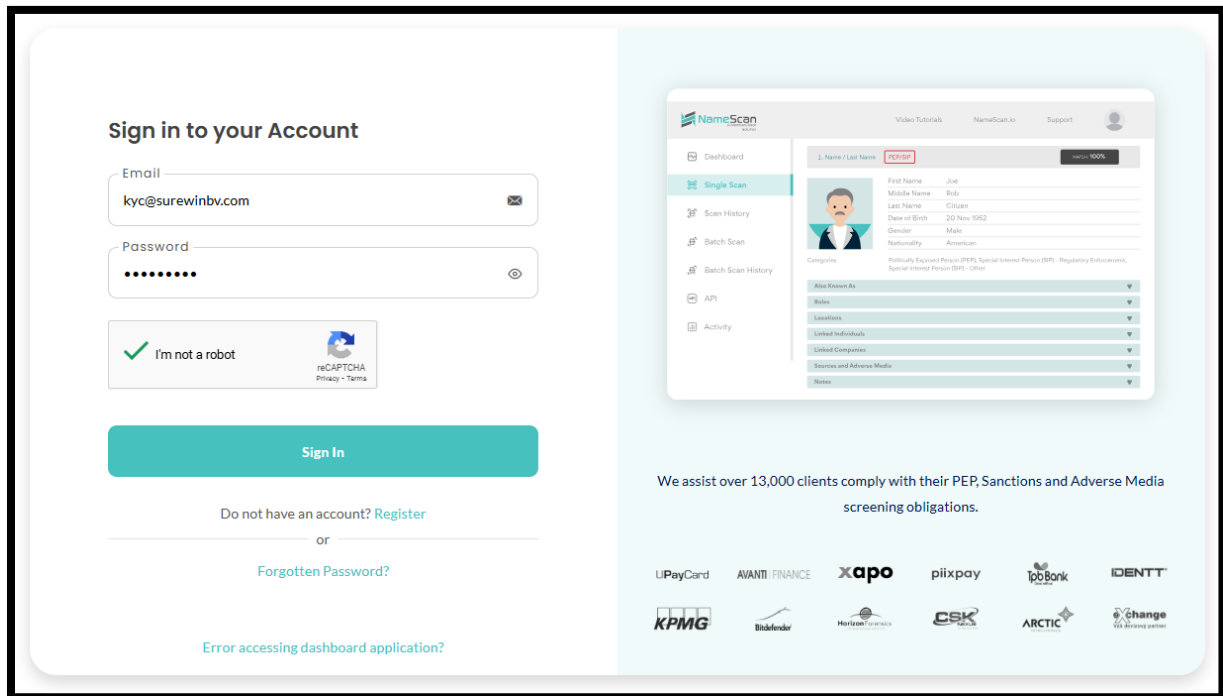
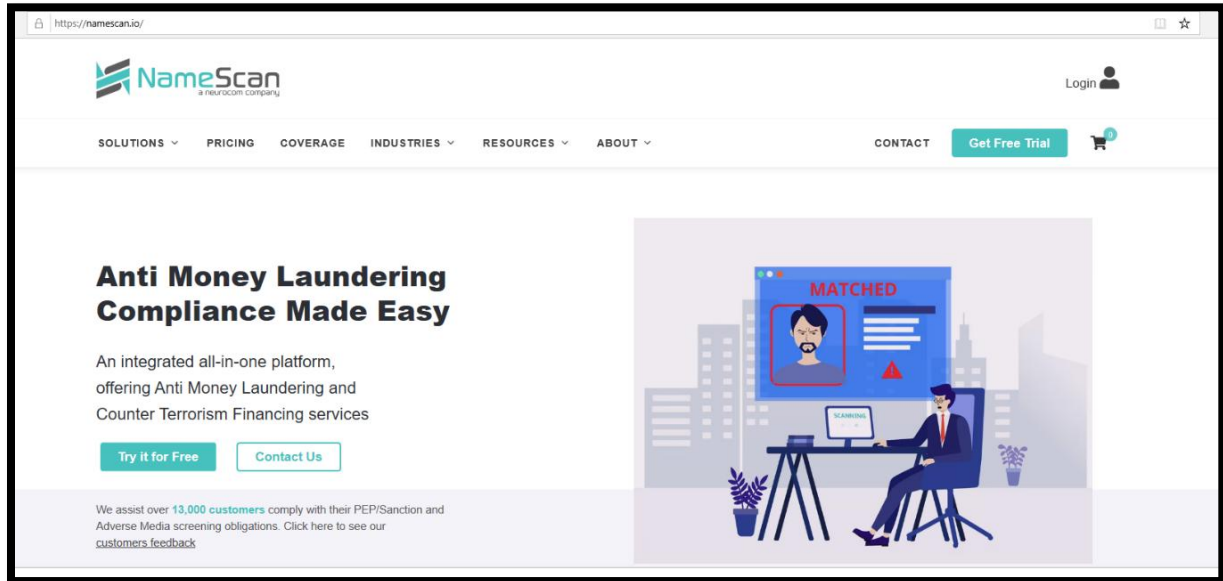
- ✓ Results will be categorized by relevance and risk level
- ✓ Review any matches carefully:
- ✓ False Positives: No action needed
- ✓ Potential Matches: Flag for further review or escalate to compliance.

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





[Sign out](#)
kyc@surewinbv.com



[SOLUTIONS](#)
[PRICING](#)
[COVERAGE](#)
[INDUSTRIES](#)
[RESOURCES](#)
[ABOUT](#)
[CONTACT](#)


English (EN)

Dashboard

Protect Your Business with Advanced PEP, Sanctions & Adverse Media Solutions

We help firms comply with AML/CTF and sanctions regulations and reduce their reputational risk by providing KYC and KYB screening solutions.

Scan Now

Contact Us



Select Screening Solutions:

- PEP Check
- Sanctions Check
- Compromised Information Check
- Media Monitoring
- ID Verification
- Jurisdiction Risk
- Biometric Verification



Trusted Individual

SINGLE SCAN

Assisted over 27,000 customers across 195 countries

FIRST NAME

Craig

ORGANISATION NAME

Surewin

VAT NUMBER

ADDRESS

CITY / TOWN / SUBURB

POSTCODE / ZIP

COMPANY SIZE

1 - 10

HOW DID YOU HEAR ABOUT US?

Other

TIME ZONE

The time on your scan history and scan report will be displayed according to your time zone setting

☒ I WANT TO RECEIVE EMAIL NOTIFICATIONS OR UPDATES

LAST NAME

Murugan

ORGANISATION REGISTRATION NUMBER

CONTACT NUMBER

1234567890

ADDRESS CONTD

STATE

COUNTRY

Cyprus

INDUSTRY TYPE

Other

Craig Murugan

kyc@surewinbv.com

My Profile

Password & Security

Order History

Settings

Dark Mode ☐

Logout

Update

Person

Organisation

Organisation and User-declared Beneficial Owners

Source

Please select the data source for this scan.

Emerald

Sapphire

Scan Settings

List Type: All

Sanction List: ALL

FATF Jurisdiction Risk: On

Adverse Media: On (Google, Bing)

Match Rate: > 25

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

Middle Name

Last Name

ROBERT

GABRIEL

MUGABE

Date of Birth

Country

Gender

21/02/1924

Zimbabwe

Male

Email Address

Record Due Diligence Decisions

Reference Number

Scan

Clear

Program

ZIMBABWE

Identities

3) Robert Mugabe

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

Reference

Consolidated PEP List

Father

Gabriel Mugabe Matibiri

Mother

Amai Bona Mugabe

Spouse

Grace Mugabe

Children

Bona Mugabe

Michael Nhamodzenyika Mugabe

Chatunga Bellamine Mugabe

Robert Peter Mugabe Jr.

Sibling

Sabina Mugabe

Citizenship

Zimbabwe

Occupations

politician

Other Names

Political Parties

Roles

Other Information

Surewin B.V recognizes the increased risk in dealing with PEP's and their associates. In addition, Surewin B.V recognizes 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 people. These are people in power and could be susceptible to corruption.

Surewin B.V has a process through which all customers are checked and screened against a PEPs/Sanctions database.

52

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 customer 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).

11.3 PEP RISK ASSESSMENT

Upon identification of a PEP the level of risk that they pose must be assessed. To do so meaningfully the following factors will be considered:

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

11.4 ONGOING MONITORING OF PEP SCREENING

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

11.5 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 customers' 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. 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.

12. 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.

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 1–2 years
 - **Standard-risk:** Every 2–3 years

Trigger Events - CDD is reapplied if:

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

12.1 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).

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

12.2 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.

12.3 RECORDKEEPING

CDD documentation will be retained for ten (10) years.

12.4 THE TERMINATION OF THE BUSINESS RELATIONSHIP

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 a 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, indicated in script/instructions accompanying the funds that these are being remitted due to the customers' inability to complete CDD.

12.5 RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE.

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

13. REPORTING OF UNUSUAL TRANSACTIONS.

Surewin B.V will maintain policies, procedures, systems, and internal controls to ensure the effective identification, monitoring, assessment, escalation, documentation, and reporting of unusual transactions in accordance with applicable Curaçao AML/CFT legislation, including the National Ordinance on the Reporting of Unusual Transactions (NORUT), applicable AML/CFT regulations, and Curaçao Gaming Authority (CGA) requirements.

The Company will ensure that:

- All directors, officers, management, employees, and relevant personnel are aware of their obligation to identify and internally report unusual transactions and suspicious activities;
- Internal reporting procedures are clearly documented and accessible to all employees;
- Employees report any unusual transaction or activity immediately to the Money Laundering Reporting Officer (MLRO);
- The MLRO has unrestricted access to customer information, transaction records, KYC documentation, source of funds information, and any other information necessary to conduct an assessment;
- The MLRO determines whether a transaction requires reporting to FIU Curaçao through the designated reporting platform without undue delay;
- All internal reports, assessments, external disclosures, investigations, supporting documentation, and decisions are appropriately documented and retained in accordance with record retention requirements;
- Staff receive ongoing AML/CFT training on the recognition and reporting of unusual transactions.

Recognition of Unusual Transactions

Surewin B.V will apply both objective and subjective indicators when identifying unusual transactions.

A transaction may consist of:

- A single completed transaction;
- An intended transaction;
- A linked series or pattern of transactions;
- Multiple transactions that collectively indicate unusual or suspicious activity.
- Linked transactions will be aggregated where required to determine whether applicable thresholds or indicators are met.

Objective Indicators

The following transactions or intended transactions will be deemed unusual under objective indicators:

- a) Transactions reported to the Police or judicial authorities in connection with money laundering, terrorist financing, or proliferation financing;
- b) Transactions conducted by or on behalf of a natural person, legal person, group, or entity appearing on applicable sanctions lists established under relevant sanctions legislation;
- c) Transactions equal to or exceeding NAf 5,000 (or the equivalent in another currency), regardless of payment method, including electronic, non-physical, or cash-equivalent transactions.

Examples include but are not limited to:

- Deposits or withdrawals equal to or exceeding the applicable threshold;
- Multiple linked transactions structured to avoid reporting thresholds;
- Transfers between payment instruments or accounts;
- Cash-equivalent transactions and payment processing activity;
- Any transaction meeting regulatory threshold requirements.

Subjective Indicators

Regardless of transaction value, a transaction will be considered unusual where there is reason to suspect that the transaction may be connected to money laundering, terrorist financing, proliferation financing, fraud, or other criminal conduct.

Examples include but are not limited to:

- Significant deposits followed by limited or no gameplay and rapid withdrawal requests;
- Unusual changes in transaction patterns or gaming activity;
- Activity inconsistent with the customer's known profile, source of funds, source of wealth, or historical behaviour;
- Attempts to avoid customer due diligence requirements;
- Reluctance or refusal to provide identification or supporting documentation;
- Multiple payment methods, accounts, or instruments without reasonable explanation;
- Structuring or fragmentation of transactions to avoid reporting thresholds;
- Transactions lacking an apparent economic or lawful purpose;
- Any transaction or behaviour that creates suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.

Internal Escalation and Reporting Process

Where an employee identifies an unusual transaction or activity, the employee will immediately submit an internal report to the MLRO and provide all relevant supporting documentation.

The MLRO will:

- Review the information and conduct further investigation where required;
- Assess whether the transaction meets objective or subjective indicators;
- Determine whether an external Unusual Transaction Report (UTR) is required;
- Submit reportable transactions to FIU Curaçao without undue delay;
- Document the rationale where an internally escalated transaction is not externally reported.
- Employees are strictly prohibited from informing customers or third parties that an unusual transaction report has been filed or may be filed.

Record Retention

All unusual transaction records, internal reports, investigations, decisions, supporting evidence, and external submissions will be retained for a minimum of five (5) years or longer where required by applicable law or regulatory obligations.

13.1 RECOGNITION OF UNUSUAL TRANSACTIONS

During ongoing monitoring activity or registration an unusual activity may be identified as 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.

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

13.2 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. The UTR must be completed in full capacity of as much information included as possible 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.

13.4 REPORTING TIMEFRAMES AND ESCALATION RESPONSIBILITIES

Reporting Timelines — Internal Escalation to MLRO

All employees who identify, detect, or are notified of unusual or suspicious activity must escalate the matter to the MLRO without delay and in any event no later than the same business day on which the concern arises.

Internal escalation must be made by completing an Unusual Transaction Report (UTR) form in full and submitting it to the MLRO without delay through the designated internal reporting channel. The UTR must include:

- The identity of the customer concerned;
- A full description of the transaction or activity giving rise to concern;
- The date(s) and amount(s) involved;
- The indicator(s) objective or subjective — that triggered the report;
- Any supporting documentation or transaction records; and
- The name and role of the reporting employee.

FIU Reporting Timelines and Escalation Responsibilities

- Internal escalation to MLRO: within 24 hours of detection.
- MLRO assessment: within 48 hours of escalation.
- UTR submission to FIU Curaçao: within 5 business days of MLRO confirmation.

Reporting Timelines — MLRO Assessment

Upon receipt of an internal UTR, the MLRO will:

Action	Deadline	Notes
Acknowledge receipt of internal UTR	Same business day	Written acknowledgement issued to reporting employee. Receipt is confidential and must not be shared with others.
Complete initial review	Within 24 hours of receipt	Determine whether the matter requires immediate account action (freeze/suspend) or can proceed under standard review.
Complete full assessment and reach a determination	Within 5 business days of receipt	Where the matter is complex or additional information is required, the MLRO may extend this period by a further 5 business days. Extension must be documented.
Submit UTR to FIU Curaçao (where warranted)	As soon as practicable and without delay once determination is made	The LMOT does not specify a fixed calendar deadline for external reporting; the obligation is to report “without delay. Surewin B.V interprets this as within 5 business days of the MLRO’s determination, absent exceptional circumstances.
Objective indicator identified (mandatory reporting)	Same business day if possible; no later than next business day	Objective indicators trigger mandatory reporting to the FIU regardless of whether suspicion exists. No internal deliberation period applies.

Where the MLRO determines that a report is not required, the rationale for that determination must be recorded in writing in the UTR register. A decision not to report is a formal decision and must be documented with the same rigor as a decision to report.

ESCALATION RESPONSIBILITIES

The escalation hierarchy is as follows:

Role	Escalates To	Responsibility
Frontline / Risk Staff	MLRO	Identify unusual or suspicious activities and submit internal UTR without delay or on the same business day.
MLRO	FIU Curaçao	Review all internal UTRs, make external disclosure decisions, submit UTRs to FIU, maintain UTR register, and report outcomes to Compliance Officer and Board.
MLRO	Compliance Officer / Board	Escalate cases of systemic concern, high-value suspicious activity, or regulatory enquiries to the Compliance Officer and Board without delay.
Compliance Officer	Board / CGA	Where the MLRO is unavailable or is the subject of concern, the Compliance Officer assumes UTR responsibilities and may escalate directly to the Board and the CGA.

TIPPING-OFF PROHIBITION

No employee, officer, or third party associated with Surewin B.V may disclose to any customer, counterparty, or external party that a UTR has been submitted, whether an investigation is underway, or that a decision to report to the FIU is being considered. Breach of this prohibition may constitute a criminal offence under applicable law and will result in immediate disciplinary action.

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.

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.

All records relating to unusual transaction monitoring, investigations, internal reports, UTRs, external disclosures, supporting documentation, MLRO assessments, FIU correspondence, and competent authority enquiries will be retained for a minimum period of five (5) years from the date of the transaction, the end of the business relationship, or the completion of the investigation, whichever is later.

Records will sufficiently demonstrate compliance with AML/CFT obligations and will be made available to the Curaçao Gaming Authority, the FIU Curaçao, and other competent authorities upon request.

Access to the registers is restricted to the MLRO, the 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 for the MLRO.
- External disclosures - ML/FT/PF/Sanctions disclosures made to the FIU or intelligence disclosures
- 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.

14. RECORD KEEPING

Surewin B.V is obliged to maintain adequate records to demonstrate compliance with its AML/CTF obligations under the LID, LMOT, CGA AML/CFT Regulations, and applicable international standards. The following retention standards apply to all categories of AML/CTF records.

14.1 MINIMUM RETENTION PERIOD

All records listed below will be retained for a minimum period of five (5) years from the later of:

- The date on which the transaction was completed or attempted;
- The date on which the business relationship ended; or
- The date on which an investigation or enquiry was formally closed.

All records related to CDD, UTRs, and transaction monitoring must be retained for a minimum of 5 years, extended to 10 years where required by law.

Where Surewin B.V applies a longer retention period (e.g. 10 years for CDD records), that longer period takes precedence. The five-year period is the regulatory minimum, and no record category may be retained for less than this period.

Record Categories and Retention Schedule

Record Category	Minimum Retention
Customer identification and KYC documents	10 years from end of relationship
Customer risk assessments	10 years from end of relationship
Source of funds/wealth assessments	10 years from end of relationship
Transaction records	5 years from transaction date
Unusual transaction monitoring records	5 years from transaction date or end of investigation
Internal UTR reports	5 years from date of report
External UTR disclosures	5 years from date of disclosure
MLRO assessments and UTR register	5 years from date of determination
Sanctions screening records - Retention of sanctions screening records supports compliance with the Sanctions National Ordinance (N.G. 2014, no. 55) and the Kingdom Sanction Act (N.G. 2016, no. 54)	5 years from screening date
FIU correspondence	5 years from date of correspondence
AML/CTF training records	5 years from training date
Independent audit reports	5 years from report date

14.2 FORMAT AND ACCESSIBILITY

All records will be maintained in a format that:

- Is accessible and retrievable within a reasonable timeframe (no longer than five (5) business days for regulatory requests);
- Cannot be altered after the record has been finalised without an auditable record of the change;

- Is protected against unauthorised access through appropriate system access controls; and
- Can be produced in a legible and intelligible format for regulatory inspection or legal proceedings.

Data protection/privacy - All records are retained in compliance with applicable data protection and privacy laws, ensuring confidentiality and lawful processing.

Access and Confidentiality

Retention practices are aligned with FIU Curaçao guidance to ensure timely production of records for investigations and enquiries

Access to AML/CTF records is restricted to the MLRO, the Compliance Officer, and the Board of Directors. Regulatory authorities including the CGA and FIU Curaçao will be granted access to all relevant records upon lawful request without delay.

The UTR register and external disclosure register are restricted to the MLRO alone, unless the Compliance Officer or Board is required to access them in an oversight capacity. Under no circumstances may these registers be accessed by operational staff or by any person who could be the subject of a report contained within them.

15. OBJECTIVE AND SUBJECTIVE INDICATORS

Surewin B.V recognises both objective and subjective indicators of unusual transactions in accordance with the Landsverordening Melden Ongebruikelijke Transacties (LMOT).

Objective Indicators are transactions that meet specific criteria prescribed by applicable laws, regulations, or guidance issued by the FIU Curaçao. Such transactions must be reported regardless of whether there is a suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.

Subjective Indicators arise where Surewin B.V knows, suspects, or has reasonable grounds to suspect that a transaction, attempted transaction, or customer activity may be connected to money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, or other criminal conduct.

The subjective indicators and red flags contained within this policy will be used to identify activity requiring further investigation and possible reporting to the MLRO.

Objective and Subjective Indicators of Unusual Transactions

In accordance with the Landsverordening Melden Ongebruikelijke Transacties (LMOT), Surewin B.V will identify and report unusual transactions based on both objective and subjective indicators.

Objective Indicators

Objective indicators are transactions that are deemed unusual by law, regulation, or guidance issued by the Financial Intelligence Unit (FIU) Curaçao and must be reported regardless of whether there is a suspicion of money laundering, terrorist financing, proliferation financing, or other criminal activity.

Examples of objective indicators include:

- Transactions meeting or exceeding applicable reporting thresholds;
- Transactions involving persons, entities, or jurisdictions subject to sanctions measures;
- Transactions specifically designated as reportable by competent authorities; and
- Any other transaction falling within a prescribed objective reporting requirement.

Where an objective indicator is met, the transaction will be reported to the FIU Curaçao without delay, irrespective of whether the company has formed a suspicion regarding the transaction.

Subjective Indicators

Subjective indicators arise where Surewin B.V knows, suspects, or has reasonable grounds to suspect that a transaction, attempted transaction, or customer activity may be related to money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, or other criminal conduct.

Examples of subjective indicators include:

- Customer behaviour inconsistent with the known customer profile;
- Unexplained or unverifiable Source of Funds or Source of Wealth;
- Structuring or attempts to avoid monitoring or reporting thresholds;
- Unusual, complex, or economically irrational transaction patterns;
- Suspicious gambling behaviour, including significant deposits with minimal wagering activity;
- Use of multiple payment methods or third-party payment instruments without a legitimate explanation;
- Adverse media, criminal allegations, or other negative information concerning the customer;
- Attempts to circumvent customer due diligence requirements; and
- Any activity that lacks an apparent lawful or economic purpose.

Transactions identified through either objective or subjective indicators will be subject to appropriate review and, where required, escalation to the MLRO for consideration of an Unusual Transaction Report (UTR) to the FIU Curaçao.

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
- Standardized inconsistent processes to meet regulatory requirements
- Removed bias from customer risk assessments
- Fulfills documentation requirements for audits
- Ensures document validity

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.

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 customer is playing on behalf of somebody else will 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 will 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 will be carried out through methods that have a money trail, i.e. methods of electronic payment only the product will 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 though 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.

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 customers will be as follows:

- PEP
- High net worth individuals
- Reactivated accounts after long periods of dormancy
- Suspicious transaction pattern
- Multiple revenue streams
- Multiple casino customer 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 high-risk jurisdiction

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

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

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 $\geq$ four thousand NAf 4,000 (€2,000 Euro) --- High Risk
- Non-face-to-face & Deposits < four thousand NAf 4,000 (€2,000 Euro) --- Standard Risk

Transaction Risk

It is important to note that due to the current anti-money-laundering and funding of terrorism regulations, the customer may deposit money only to play and use our services.

Likewise, the customer 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 customers upon reach:

- Four thousand NAf 4,000 (€2,000 Euro) threshold in deposits
- E-Wallets – 1,000 NAf (€500 Euro) or more deposits in the last 2 months;
- More than 3 payment instruments used in the last 72 hours;
- Threshold 20,000 NAf (€10k Euro) in 7 days;
- Threshold 30,000 NAf (€ 15k Euro) in 30 days.

Technological Development 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 reviewed:

- Whenever a new product is developed;
- A new delivery mechanism is becoming available;
- A new business practice emerges, in particular every time money and technology come together in a new way or
- 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 recognized 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 is maintained in order to demonstrate its basis and how they are reviewed.

Independent Audit Function

Surewin B.V will maintain an independent audit function to test the effectiveness of its AML/CFT program annually. Audit findings will be reported to the Board of Directors and MLRO, and corrective actions will be implemented promptly.

CGA Examination

The Curaçao Gaming Authority (CGA) may conduct examinations of Surewin B.V AML/CFT compliance program. The company commits to full cooperation, including provision of records, reports, and staff interviews during such inspections.

Formal Approval

This AML/CFT Policy is formally approved by:

- Compliance Officer
- Managing Director

17. 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 analyzed 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.

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 from 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.

18. 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.

19. 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.

20. 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 will be appropriately tailored to Surewin B.V 's activities and will 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 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.

21. AML/CFT AUDIT AND ASSURANCE FRAMEWORK

Surewin B.V will maintain an independent, risk-based AML/CFT Audit Framework designed to provide the Board of Directors and Senior Management with reasonable assurance that the AML/CFT compliance programme remains effective, proportionate and compliant with all applicable Curaçao legislation, CGA requirements and internal policies.

The framework forms the Company's third line of assurance and is intended to independently evaluate the design, implementation and operating effectiveness of the AML/CFT control environment.

The AML/CFT audit will be performed by suitably qualified personnel who are independent from the operational activities being audited.

The auditor may be:

- an Internal Audit function;
- an independent Compliance Assurance function;
- an external audit firm; or
- another suitably qualified independent person approved by the Board.

Persons responsible for day-to-day AML operations, customer onboarding, transaction monitoring or MLRO decision-making shall not audit their own activities.

A full AML/CFT audit shall be performed at least annually.

Additional targeted reviews will be conducted whenever:

- significant regulatory changes occur;
- new products or payment methods are introduced;
- material AML incidents occur;
- deficiencies are identified by regulators;
- significant control failures are identified; or
- the MLRO or Board considers additional assurance necessary.

21.1 RISK-BASED AUDIT PLANNING

The annual AML Audit Plan will be approved by the Board of Directors (or a delegated Board Committee).

Planning will consider:

- enterprise AML risk assessment;
- customer risk profile;
- transaction volumes;
- high-risk jurisdictions;
- payment methods;
- outsourcing arrangements;
- previous audit findings;
- regulator feedback;
- new legislation;

- changes to systems or products; and
- emerging money laundering typologies.

21.2 MINIMUM AUDIT SCOPE

Each annual audit will assess, where applicable:

- AML governance arrangements;
- Board oversight;
- MLRO effectiveness;
- AML Risk Assessment;
- Customer Acceptance procedures;
- Customer Due Diligence (CDD);
- Enhanced Due Diligence (EDD);
- Source of Funds procedures;
- Source of Wealth procedures;
- PEP controls;
- Sanctions screening;
- Linked transaction detection;
- Transaction monitoring;
- Unusual Transaction reporting;
- goAML reporting;
- Record retention;
- Staff training;
- Quality Assurance;
- Third-party reliance;
- Outsourcing oversight;
- Technology controls;
- System access controls;
- Data integrity;
- Management reporting;
- Regulatory reporting; and
- Effectiveness of remediation from previous audits.

21.3 AUDIT METHODOLOGY

The audit will include, where appropriate:

- policy review;
- document review;
- customer file testing;
- transaction testing;
- walkthroughs;
- sampling;
- interviews;
- control testing;
- system testing;
- observation of operational processes;
- review of management information;
- review of regulatory reporting; and
- testing of remediation evidence.

21.4 AUDIT RATING

Each finding will be assigned:

- Critical
- High
- Medium
- Low

based on:

- regulatory impact;
- financial crime exposure;
- customer impact;
- operational impact; and
- likelihood of recurrence.

21.5 REMEDIATION

Each audit finding will include:

- finding reference;
- root cause;
- risk rating;
- corrective action;
- responsible owner;
- target completion date;
- actual completion date;
- evidence of closure; and
- management validation.

21.6 AUDIT REPORTING

The final audit report will be submitted to:

- Board of Directors;
- Managing Director;
- Compliance Officer;
- MLRO; and
- other relevant Senior Managers.

The report shall include:

- executive summary;
- overall assurance opinion;
- findings;
- observations;
- recommendations;
- management responses;
- remediation status; and
- residual risk assessment.

21.7 BOARD OVERSIGHT

The Board shall:

- review the annual AML audit plan;
- review audit results;
- challenge management where appropriate;
- monitor remediation progress;
- approve closure of critical findings; and
- ensure sufficient resources exist to maintain an effective AML programme.

21.8 CONTINUOUS ASSURANCE

Between formal annual audits, Surewin B.V will perform ongoing AML assurance through:

- Compliance monitoring;
- Quality Assurance reviews;
- MLRO oversight;
- KPI monitoring;
- Targeted reviews;
- trend analysis;
- regulator feedback reviews;
- incident reviews; and
- management self-assessments.

21.9 AUDIT RECORDS

Surewin B.V will maintain:

- Annual Audit Plans;
- Working papers;
- Audit reports;
- Remediation logs;
- Board papers;
- Management responses;
- Evidence of closure; and
- Historical audit records.

All audit documentation shall be retained for a minimum of five (5) years or longer where required by applicable law or regulatory instruction.

22. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Compliance Obligation

All employees, managers, third-party partners, and affiliates of Surewin B.V are required to comply with the company's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy and related procedures. Full adherence to these obligations is not only a matter of company policy but also a legal requirement under Curaçao's AML/CFT framework, including the Landsverordening Identificatie bij Dienstverlening (LID), Landsverordening Melding Ongebruikelijke Transacties (LMOT), and relevant CGA Directives.

Failure to follow these obligations exposes both individuals and the company to serious legal, regulatory, and reputational risks.

Risks of non-compliance

Violations of the AML/CFT Policy can result in:

Legal and Regulatory Penalties

- Regulatory sanctions from the Curaçao Gaming Authority (CGA), including license suspension or revocation
- Fines or penalties issued by the Financial Intelligence Unit (FIU Curaçao)
- Criminal liability under Curaçao AML laws for employees and executives involved in wilful or negligent violations

Reputational Damage

- Loss of trust among customers, partners, and investors
- Public disclosure of enforcement actions leading to market loss

Operational Risks

- Freezing of assets or account closures by payment providers or banks
- Disruption of business continuity or service availability
- Loss of key partnerships or access to payment networks

Internal Disciplinary Measures

In addition to external legal consequences, Surewin B.V may take the following internal disciplinary actions for violations of this AML/CFT policy:

- Verbal or written warnings
- Mandatory retraining or suspension from duties
- Formal reprimands placed in personnel records
- Temporary suspension or termination of employment or contracts
- Contract termination with external vendors or affiliates

Reporting Violations

All employees and stakeholders have a duty to report suspected violations of this policy. Reports should be made directly to the Money Laundering Reporting Officer (MLRO) or through other designated internal reporting channels. Surewin B.V prohibits retaliation against any employee or third party who, in good faith, reports a suspected AML/CFT violation.

Commitment to Enforcement

Surewin B.V is fully committed to enforcing this AML/CFT policy consistently and fairly. All violations will be investigated thoroughly, and disciplinary or corrective action will be taken in accordance with internal procedures and applicable laws.

Related Information

This section lists the key legal instruments, regulatory guidelines, internal policies, and supporting documents that inform and support the implementation of Surewin B.V AML/CFT compliance framework.

Legal and Regulatory Frameworks:

Landsverordening Identificatie bij Dienstverlening (LID) National ordinance on customer identification requirements.

Landsverordening Melding Ongebruikelijke Transacties (LMOT) – National ordinance on the reporting of unusual transactions.

Curaçao Gaming Authority (CGA) AML/CFT Regulations (Effective January 2025) – Binding AML/CFT framework for all licensed gaming operators.

FATF Recommendations – International standards on combating money laundering, terrorist financing, and proliferation financing. <https://www.fatf-gafi.org/recommendations.html>

Sanctions Lists and Guidance

OFAC Sanctions List: <https://sanctionssearch.ofac.treas.gov>

UN Sanctions List: <https://www.un.org/securitycouncil/sanctions/un-sc-consolidated-list>

EU Sanctions Map: <https://www.sanctionsmap.eu>

Contact Information

For any questions regarding this policy, please contact: Insert name/office, phone number, and email address.

Policy History

Indicate whether this is a new policy or if it replaces an existing one. List previous versions with effective dates and revisions, if applicable.

Policy URL (if applicable)

Indicate where the policy can be accessed online if published on the Company website.

Policy Approval

This AML/CFT Policy has been reviewed and approved by senior management and is effective from the date stated below.

Position	Name	Signature	Date
Managing Director			
Compliance Officer	Craig Murugan		29 June 2026

By signing this document, the undersigned confirm their commitment to ensuring that the company maintains an effective AML/CFT framework and complies with all applicable legal, regulatory, and licensing obligations.