

**WhiteBox B.V.**  
Korporaalweg 10, Willemstad,  
Curaçao

# **WhiteBox B.V.**

## **AML Policy and Procedures**

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

## **HISTORY OF CHANGES**

| <b>Date</b> | <b>Ver.</b> | <b>Author</b>       | <b>Summary Changes</b>                      |
|-------------|-------------|---------------------|---------------------------------------------|
| 01.03.2024  | 1.0         | WhiteBox Group B.V. | First Version                               |
| 19.02.2025  | 2.0         | WhiteBox Group B.V. | New version of ANTI-MONEY LAUNDERING MANUAL |
| 03.04.2025  | 3.0         | WhiteBox Group B.V. | New version of ANTI-MONEY LAUNDERING MANUAL |
| 21.05.2025  | 4.0         | WhiteBox Group B.V. | New version of ANTI-MONEY LAUNDERING MANUAL |
| 20.05.2026  | 4.1         | WhiteBox Group B.V. | New version of ANTI-MONEY LAUNDERING MANUAL |

**Note:** This policy is subject to review at least once every 12 months or upon any material change in regulatory obligations, operational processes, or identified risks.

**Next Scheduled Review:** 20.05.2027

**Contact information:**

**Name:** Christine Nicholls

**Position:** Money Laundering Reporting Officer (MLRO)

**Phone:** +599 9 843 0012

**Email:** compliance@xcm.cw

# Whitebox B.V.

## AML Policy and Procedures

Version 4.1

### Table of Contents

|                                                           |    |
|-----------------------------------------------------------|----|
| 1. AML Management Overview .....                          | 5  |
| 1.1. Purpose .....                                        | 5  |
| 1.2. Policy Statement and Audience .....                  | 6  |
| 1.3. Definitions .....                                    | 8  |
| 1.4. Business Risk Assessment & Risk-Based Approach ..... | 10 |
| 1.5. Data processing system .....                         | 13 |
| 1.6. Staff Training .....                                 | 13 |
| 2. Customer Acceptance and Registration Policy .....      | 15 |
| 2.1. Introduction .....                                   | 15 |
| 2.2. Customer Acceptance .....                            | 15 |
| 2.3. Restrictions .....                                   | 15 |
| 2.4. Information Entered on Registration .....            | 16 |
| 2.5. Terms Acceptance .....                               | 17 |
| 2.6. Underage Customers .....                             | 17 |
| 2.7. Customer Due Diligence .....                         | 17 |
| 3. Customer Risk Scoring and Profiling .....              | 18 |
| 3.1. Introduction .....                                   | 18 |
| 3.2. Customer Risk Assessment .....                       | 18 |
| 3.2.1. Individual status .....                            | 19 |
| 3.2.2. Geographical location .....                        | 20 |
| 3.2.3. Gambling and transactional behaviour .....         | 20 |
| 3.2.4. Payment Methods .....                              | 20 |
| 3.2.5. Fraud red flags .....                              | 21 |
| 3.3. Risk Score Calculation .....                         | 21 |
| 3.4. Customer Due Diligence level .....                   | 23 |
| 3.5. Additional Details & Source of Funds/Wealth .....    | 24 |
| 3.6. On-Going Monitoring .....                            | 24 |
| 3.7. Withdrawals .....                                    | 24 |
| 4. Customer Due Diligence .....                           | 26 |
| 4.1. Introduction .....                                   | 26 |
| 4.2. Standard Customer Due Diligence .....                | 26 |
| 4.3. Documents acceptance .....                           | 27 |

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

|      |                                                     |    |
|------|-----------------------------------------------------|----|
| 4.4. | Threshold approach                                  | 27 |
| 4.5. | Ongoing monitoring                                  | 28 |
| 4.6. | Enhanced Due Diligence                              | 29 |
| 4.7. | Politically Exposed Persons and Sanctions Screening | 31 |
| 4.8. | Procedure for Account Closure                       | 33 |
| 5.   | Deposit and Withdrawal Management Procedures.....   | 34 |
| 5.1. | Player Account Balance                              | 34 |
| 5.2. | Payment Methods                                     | 34 |
| 5.3. | Player Deposits                                     | 34 |
| 5.4. | Player Withdrawals                                  | 35 |
| 5.5. | Withdrawal Payouts                                  | 35 |
| 5.6. | Verification and Conditions                         | 35 |
| 6.   | Suspicious and Unusual Activity Reporting .....     | 36 |
| 6.1. | Introduction                                        | 36 |
| 6.2. | Red Flags Indicators                                | 36 |
| 6.3. | Inability to Complete CDD Measures                  | 37 |
| 6.4. | Internal Unusual Transaction Report (Internal UTR)  | 37 |
| 6.5. | External report to FIU                              | 38 |
| 6.6. | Reporting Procedure via goAML                       | 38 |
| 6.7. | Tipping-off                                         | 39 |
| 7.   | Internal Control .....                              | 40 |
| 7.1. | Introduction                                        | 40 |
| 7.2. | Employees background check                          | 40 |
| 7.3. | Record keeping                                      | 40 |
| 7.4. | Money Laundering Reporting Officer                  | 41 |
| 7.5. | Training                                            | 43 |
| 7.6. | Internal revision and staying up to date            | 44 |
| 8.   | Compliance and Consequences of Non-Compliance.....  | 46 |

# 1. AML Management Overview

## 1.1. Purpose

WhiteBox B.V., a limited liability company incorporated under the laws of Curaçao, with the company number 155412, having its registered office at Korpuraalweg 10, Willemstad, Curaçao (hereinafter – the Company), has developed current AML Manual in accordance with the applicable legislation of the EU and Curaçao, reports of Financial Action Task Force and International standards of money laundering prevention, in particular (but not limited to):

- National Ordinance on Games of Chance (LOK) (Landsverordening op de kansspelen);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no 48);
- The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024;
- The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- National Decree Penalties and Fines Reporting Unusual Transactions (N.G. 2021, no. 69), as amended by PB 2023, no. 6;
- National Decree supervisor identification when rendering services gaming sector (L.B. 28.01.2019, no. 19/0282);
- National Decree supervision unusual transactions gaming sector (L.B. 28.01.2019, no. 19/0283);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015, no. 30);
  - Kingdom Sanction Act (N.G. 2016, no. 54);
  - National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
  - National Ordinance extension of validity sanction decrees (N.G. 2018, no. 34);
  - National Decree Prohibition to Import, Export and Transit of Venezuelan Gold (N.G. 2019, no. 82);
  - National Ordinance on the Obligation to Report Cross-Border Money Transportation (N.G. 2002, no. 74), as amended by (N.G. 2014, no. 90);
  - National Ordinance on Offshore Games of Hazard (PB 1993, no. 63);
  - Curacao Gaming Authority, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, last update January 2025.

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

### 1.2. Policy Statement and Audience

WhiteBox B.V. is committed to preventing its systems, products, and services from being used to facilitate money laundering, terrorist financing, or any other financial crimes. Our intent is to maintain a robust, zero-

## Whitebox B.V. AML Policy and Procedures

Version 4.1

tolerance compliance framework that adheres to all applicable anti-money laundering (AML) and counter-terrorist financing (CTF) laws and regulations. This policy establishes the mandatory minimum standards for detecting, preventing, mitigating, and reporting suspicious activities across all business operations globally.

To ensure comprehensive risk management, the scope of this policy extends to all individuals and entities acting on behalf of the Company. The rules and obligations outlined within this document are mandatory for the following stakeholders:

- **All Employees:** Including the Board of Directors, executive officers, full-time, part-time, and temporary staff across all departments and global locations.
- **Subcontractors and Consultants:** Independent professionals and temporary workers engaged to perform internal or external services for the organization.
- **Third-Party Suppliers and Agents:** Vendors, brokers, partners, and external service providers who interact with customers, manage data, or process financial transactions on our behalf.
- **Subsidiaries and Affiliates:** All business units and corporate entities under the direct or indirect control.

The Compliance Officer is the key individual responsible for the prevention of money laundering and the financing of terrorism. This role encompasses overall responsibility for maintaining regulatory compliance and overseeing anti-money laundering (AML) procedures. The Compliance Officer is actively involved in defining and managing the processes necessary to prevent money laundering and other fraudulent activities, based on the following principles:

- **Risk-Based Approach:** While the Company assumes that most customers are not involved in money laundering activities, it identifies and verifies all players as required by applicable regulations, using a risk-based approach.
- **Transaction Monitoring:** The Company diligently monitors all transactions and customer activities to identify and report any suspicious behavior.
- **Continuous Monitoring:** Ongoing monitoring of customers, risks, and processes is conducted to ensure that the Company's AML and Counter-Terrorism Financing (CTF) measures remain effective and up-to-date.

Additionally, the Company is committed to ensuring that all relevant

## Whitebox B.V. AML Policy and Procedures

Version 4.1

employees receive comprehensive training on AML and CTF policies and procedures. This training emphasizes the importance of vigilance against these risks. To ensure proficiency, relevant employees are required to pass competency tests on this subject matter.

Adherence to this policy is a fundamental condition of employment and business engagement. Failure to comply with these standards will result in severe disciplinary action, up to and including termination of employment or business contracts, as well as potential civil and criminal liabilities.

### 1.3. Definitions

#### What is Money Laundering?

Money laundering (ML) refers to the process by which individuals attempt to disguise the origins of money obtained through illegal means, making it appear as though it comes from legitimate sources. This is essentially the transformation of "dirty" money into "clean" money. The process of money laundering typically involves three main stages:

1. **Placement** – This is the initial step where illegally obtained money is introduced into the financial system. This can be done through a variety of methods such as depositing cash into bank accounts, purchasing casino chips and cashing them out without significant play, using credit or debit cards, prepaid cards, checks, or cryptocurrencies to fund casino accounts, and then requesting withdrawals. Additionally, it can involve inserting cash into gaming machines and immediately converting it to credits.
2. **Layering** – In this phase, the launderer attempts to obscure the origins of the money by engaging in complex transactions. This can include transferring funds between multiple accounts, often across different financial institutions or jurisdictions, converting currencies, breaking down large amounts into smaller, less suspicious sums (known as structuring), and utilizing various gambling accounts to hide the money from law enforcement.
3. **Integration** – The final stage involves reintegrating the laundered money into the legitimate economy, making it difficult to distinguish from legal income. This is often done through investments in luxury

**Whitebox B.V.**  
**AML Policy and Procedures****Version 4.1**

goods, real estate, financial products, or even legitimate businesses, including gaming companies. By making these investments or purchases, the laundered money is effectively "cleaned" and can be used without arousing suspicion.

**What is Financing of Terrorism?**

Financing of Terrorism (FT) refers to providing funds or financial support for terrorist activities, individuals, or groups. A terrorist act is defined as an action intended to intimidate the public or coerce a government or international organization into taking or refraining from certain actions.

The key difference between terrorist financing and money laundering lies in the source of the funds. While money laundering always involves money obtained through illegal means, terrorist financing can involve money from both legal and illegal sources. The funds used for terrorism may be legally acquired, but are used for unlawful political purposes.

Terrorist groups need to obscure the connection between their activities and their funding sources. To do this, they employ methods similar to those used in money laundering. These methods include smuggling cash, breaking down large sums into smaller transactions (structuring), conducting wire transfers, buying monetary instruments, and using debit and credit cards.

While the primary concern in money laundering is to hide the origins of the illicit funds, the focus in terrorist financing is to conceal the destination or the end recipient of the funds.

The detection and deterrence of money laundering (ML) and terrorist financing (TF) are critical to maintaining the integrity and legal compliance of the company's operations. As an online casino operator, the company acknowledges the inherent risks associated with the gaming industry, which can be vulnerable to abuse by individuals seeking to launder illicit funds or finance terrorism. In accordance with applicable national and international regulations, the company is committed to implementing and maintaining effective policies and procedures designed to detect, prevent, and report suspicious activities related to ML and TF. These measures are fundamental to ensuring that the company operates within the bounds of the law, safeguards its reputation, and protects the interests of its legitimate customers. The company's efforts in combating money laundering and

**Whitebox B.V.**  
**AML Policy and Procedures****Version 4.1**

terrorist financing contribute to promoting a secure and transparent gaming environment and are essential to upholding the standards of responsible gaming.

**What is Financing of Proliferation of Weapons?**

Financing of Proliferation (FP) refers to the act of providing financial resources for the creation, acquisition, ownership, development, export, transportation, brokerage, transfer, storage, or use of nuclear, chemical, or biological weapons, as well as the materials and delivery systems associated with these weapons. This includes any funding that supports the spread and availability of these highly destructive weapons and their related components.

The company has implemented robust internal security measures to combat Money Laundering (ML), Financing of Terrorism (FT), and Financing of Proliferation of Weapons (FP). These measures are designed to identify and monitor high-risk customers and detect suspicious activities, including those related to underlying criminal activities associated with money laundering, terrorist financing, and financing of proliferation of weapons.

**1.4. Business Risk Assessment & Risk-Based Approach****What is the Risk-Based Approach?**

The risk-based approach is a fundamental element of The Company's anti-money laundering (AML) compliance program. It aims to protect the organization from money laundering and terrorist financing activities, ensuring compliance with relevant laws and regulations. This approach aligns with the Financial Action Task Force (FATF) Recommendations, which require casinos to tailor their AML measures to the specific risks they face.

**Principles of the Risk-Based Approach**

By adopting a risk-based approach, The Company ensures that measures to prevent or mitigate money laundering, financing of terrorism, and proliferation of weapons are proportional to the risks identified. This means higher risks require more stringent measures, while lower risks may be managed with simplified procedures, provided they comply with the country's AML/CTF assessments.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

### Application of the Risk-Based Approach

Applying the risk-based approach involves several key steps:

- **Risk Identification and Assessment:** Evaluate the likelihood of money laundering and terrorist financing occurring within the organization. This includes analyzing factors such as customer profiles, geographic locations, products and services offered, and transaction types.
- **Risk Mitigation:** Implement appropriate policies, procedures, and controls to manage and mitigate identified risks. This involves designing measures that are proportional to the level of risk assessed.
- **Risk Monitoring:** Continuously monitor and enhance the effectiveness of policies, procedures, and controls. This includes updating the risk profile based on changes to the business, emerging threats, and new regulatory requirements.
- **Documentation:** Maintain comprehensive documentation of risk assessments, including the rationale behind the measures implemented. This documentation should detail the policies, procedures, and controls in place and the reasons for their application.

To quantify the exact extent and likelihood of these risks, the Company maintains a comprehensive, standalone data-driven risk matrix.

**Formal Incorporation by Reference:** The localized threat matrices, specific statistical vulnerabilities, and deep-dive risk ratings are recorded in the separate, dynamic document titled *"WhiteBox B.V. - Business Risk Assessment for the Prevention of Money Laundering, Terrorist Financing and Proliferation Financing"*. This standalone document is formally incorporated into this AML Policy by reference, holds equal regulatory weight, and serves as the analytical justification for the controls outlined throughout this manual. In the creation and implementation of the AML Manual, a comprehensive risk assessment is carried out, encompassing the following categories:

- **Customer Risk:** The Company examines specific customer groups and their business relationships to identify potential risk factors that could indicate a heightened susceptibility to money laundering or terrorist financing.

## Whitebox B.V.

### AML Policy and Procedures

Version 4.1

- **Channel Risk:** The methods used to establish business relationships or conduct transactions are also considered when evaluating the overall risk profile. Channels that allow for anonymity may increase ML/TF risks unless proper safeguards are implemented.

- **Payment Method Risk:** The Company conducts reviews of the payment methods it offers, evaluating how the features of these methods could be exploited for money laundering or terrorist financing purposes.

- **Geographical Risk:** The Company analyzes the risks associated with the geographic areas where it operates. This assessment includes factors such as the local regulatory environment, the prevalence of financial crime, and vulnerabilities specific to certain jurisdictions.

- **Product Risk:** The Company reviews the features of its products to determine the extent to which they could be misused for unlawful activities, such as money laundering or the financing of terrorism. In cases where a new product is developed or when new or developing technologies are introduced, a risk assessment will be conducted prior to the launch to evaluate potential vulnerabilities and ensure that appropriate risk mitigation measures are in place.

- **Service Delivery Risk:** Risks linked to the distribution channels of the Company's services, including online platforms and mobile applications, are carefully assessed. Controls are implemented to address vulnerabilities that could facilitate money laundering or terrorist financing.

- **Employee Risk:** Risks arising from potential employee misconduct or collusion in illicit activities are also evaluated. The Company ensures that robust measures are in place to mitigate insider threats effectively.

Products capable of facilitating large, rapid, or anonymous transactions, or those susceptible to manipulation, are classified as higher risk and subjected to stricter controls.

To effectively manage risks associated with various gaming activities, the Company evaluates game types according to their key risk characteristics. Slot machines are assessed as low risk due to their fixed outcomes and typically smaller transaction amounts. Table games and sports betting present medium risk, characterized respectively by frequent, large bets and high transaction volumes. Poker and peer-to-peer games carry a high risk due to increased player interaction, anonymity concerns, potential collusion, and higher stakes involved.

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

## **1.5. Data processing system**

The Company utilizes an advanced internal data processing system to detect high-risk scenarios, money laundering, and terrorist financing in its day-to-day operations. This system is a crucial component of the Company's AML/CFT/CFP framework.

The data processing system incorporates the following mechanisms to ensure effective monitoring and compliance:

- **User Identification and Verification:** Before establishing any business relationship, all users undergo thorough identification and verification processes carried out by internal Know Your Customer (KYC) software integrated into the company's website.
- **Politically Exposed Person (PEP) and Sanction List Checks:** The system performs checks against PEP and sanctions lists using specialized software to ensure compliance with relevant regulations.
- **Transaction Monitoring:** Trained staff manage transaction monitoring through internal transaction monitoring software. This software continuously analyzes transactions to identify and flag suspicious activities.
- **Reporting Suspicious Activities:** All suspected cases of money laundering are promptly reported to the Compliance Officer and the Financial Intelligence Unit (FIU).

The Company is committed to continuously monitoring trends and changes related to money laundering and terrorist financing. This proactive approach ensures that the data processing system remains up-to-date and effective in identifying and mitigating emerging risks.

## **1.6. Staff Training**

Upon joining The Company and annually thereafter, all staff members, including those from outsourcing teams, will receive comprehensive training on AML/CFT procedures and related policies. This training is crucial for ensuring that all employees understand their roles and responsibilities in preventing money laundering and terrorist financing.

The training will be delivered through a combination of online and face-to-face sessions. It will be conducted by professional training providers or by

**Whitebox B.V.**  
**AML Policy and Procedures****Version 4.1**

the Company's own specialists, depending on the specific requirements and circumstances. The training content will be tailored to meet the needs identified through individual risk analysis. This ensures that staff members receive relevant information and practical guidance specific to their roles and the risks they might encounter.

By implementing a thorough and ongoing training program, The Company ensures that its workforce remains informed and capable of effectively contributing to the Company's AML/CFT efforts.

## 2. Customer Acceptance and Registration Policy

### 2.1. Introduction

Before engaging in gambling, making deposits, or placing real-money bets, customers must register an account. Individuals who do not register an account will be unable to participate in gambling activities.

The Customer Acceptance and Registration Policy outlines the criteria and processes for accepting potential customers and completing their registration.

### 2.2. Customer Acceptance

To deposit funds and participate in gambling on the company's platform, a customer must first complete the registration process on the site.

Registration is restricted to individuals who are at least eighteen years old.

Each customer is allowed to open only one account in their name per site. To enforce this, additional checks are conducted to block multiple accounts using the same email address, mobile number, device, or other combinations of customer data. These measures prevent customers from creating multiple accounts to bypass AML thresholds and other regulatory requirements.

The Company does not permit users to open or operate anonymous accounts or accounts registered under obviously fictitious names. In line with AML/CFT regulations, every user must complete the required identity verification process before being allowed to deposit funds, access gaming services, or engage in any financial activity on the Website.

### 2.3. Restrictions

The Company imposes several restrictions to ensure compliance with AML regulations and maintain a secure gaming environment. The following individuals are not permitted to register on the site:

- **Underage Individuals:** Persons under 18 years of age are strictly prohibited from registering;

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- **Politically Exposed Persons (PEPs) and Sanctioned Individuals:** Individuals identified as PEPs, those under sanctions, or those listed on any blacklists are not allowed to register. This includes, but is not limited to, those listed under the following sanction lists:
  - Consolidated United Nations Security Council Sanctions List
  - Consolidated list of persons, groups and entities subject to EU financial sanctions
  - Office of Foreign Assets Control Sanctions List
  - Her Majesty's Treasury Sanctions List
  - Sanction Decree "Al-Qaida" (N.G. 2015, no. 29)
  - Ministerial Regulation "Libya" (N.G. 2015, 28)
  - Sanction Decree "Islamic Republic Iran 2015" (N.G. 2015, 27)
  - Sanction Decree "Democratic People's Republic of Korea 2015" (N.G. 2015, 30)
  - Ministerial Regulation "Yemen" (N.G. 2015, 65)
- **Excluded Customers:** Individuals who have been previously excluded from the site for any reason are not permitted to re-register.
- **Individuals with Fraud Red Flags:** Customers flagged for fraud or suspicious activities are prohibited from registration.

Customers are allowed to open only one account in their name per site. To enforce this, the Company conducts additional checks to block multiple accounts using the same email address, mobile number, device, or other combinations of customer data. These checks help prevent the creation of multiple accounts to bypass AML thresholds and other regulatory measures.

### 2.4. Information Entered on Registration

During the registration process, and potentially later, The Company may request the following identifying information and contact details from customers:

- First Name
- Last Name
- Date of Birth
- Gender
- Address and Country of Residence
- Email Address and Mobile Number
- Username and Password

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

## **2.5. Terms Acceptance**

As part of the registration process, customers must confirm their acceptance of the website's general terms and conditions as well as its privacy policy.

## **2.6. Underage Customers**

The system is designed to prevent the registration of underage customers. For the registration process to be successful, customers must be at least 18 years old or of legal age in their respective territories.

## **2.7. Customer Due Diligence**

To complete the registration process, customers must pass Customer Due Diligence (CDD). If a customer fails to pass the CDD, their registration will be declined.

## 3. Customer Risk Scoring and Profiling

### 3.1. Introduction

In line with the risk-based framework, WhiteBox B.V. conducts risk profiling of all customers from the moment they register to assess potential money laundering (ML) and terrorist financing (TF) risks. The Company's policies and procedures are guided by:

- Regulatory and legal requirements.
- Guidance from the Curacao Gaming Authority (CGA) and Financial Intelligence Unit (FIU).
- Internal evaluations of business risks and experiences with customers.

### 3.2. Customer Risk Assessment

Upon registration, The Company evaluates each customer to determine their risk level for ML and TF. This initial risk assessment is based on information provided during the registration process and is regularly updated as new data becomes available. Customers are categorized as Low, Medium, or High risk, influencing the level of monitoring and due diligence applied.

The risk assessment process based on:

- **Individual Status:** Assessing if the customer is a Politically Exposed Person (PEP) or listed under any sanctions.
- **Geographical Risk:** Evaluating the risk associated with the customer's country of residence.
- **Behavioral Analysis:** Monitoring gambling and transactional behaviors for signs of ML or TF.
- **Payment Methods:** Analyzing the risk associated with the methods used for deposits and withdrawals.
- **Fraud Indicators:** Identifying any red flags related to fraud or suspicious activities.

Customers who are considered High Risk will need to undergo EDD.

**Whitebox B.V.**  
**AML Policy and Procedures****Version 4.1**

The Company employs a risk-based approach to evaluate and monitor the typical transaction volumes and amounts associated with its customers. If unusual or suspicious behavior is detected, additional checks or enhanced due diligence (EDD) may be performed to confirm that the activity corresponds with the customer's profile and to address potential risks.

**3.2.1. Individual status****PEP**

A Politically Exposed Person (PEP) is someone who has been assigned a significant public function at the international, European, or national level, or who has held a prominent political position below the national level. This includes their immediate family members and close associates.

Any customer, whether new or existing, identified as a PEP or related to a PEP will have their account rejected or closed.

**Sanctions list**

Sanction lists are compiled by governments and international bodies to identify individuals, organizations, and entities involved in illegal activities. These lists aim to combat terrorism, money laundering, and other financial crimes.

Individuals and Entities on these lists are subject to financial restrictions that prevent them from accessing the international financial system.

Any new or existing customer found on these sanctions' lists will have their account rejected or closed.

**Adverse media**

Adverse media, also known as negative news, refers to any unfavorable information about a customer or business discovered through various sources. This information can indicate potential involvement in criminal activities.

Any customer mentioned in adverse media reports will be subjected to enhanced due diligence (EDD). Based on the results of the EDD, the company may decide to close the account or reject the registration.

**Whitebox B.V.**  
**AML Policy and Procedures****Version 4.1****3.2.2. Geographical location**

Customers residing in high-risk countries are flagged for EDD. High-risk countries are identified using various sources, including:

- FATF list of High-Risk Jurisdictions subject to a Call for Action
- FATF list of Jurisdictions under Increased Monitoring
- CFATF Public Statements
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

**3.2.3. Gambling and transactional behaviour**

The customer's gambling and transactional behaviour is continuously monitored to detect markers that indicate money laundering and markers of harm for problem gambling.

Detected markers affect the overall risk scoring in combination with other detected ML/TF red flags.

If any examples of overt ML/FT behaviour are observed, then an EDD must be undertaken immediately of the customer, and an Unusual Transaction Report (UTR) is filed if necessary.

**3.2.4. Payment Methods**

Payment methods that enable us to trace the origin of the funds, such as those linked to a bank account, and facilitate refunds to the original source are deemed low risk.

Conversely, payment methods funded by cash, which do not allow us to trace the source of the funds or return them to the original source, are considered high risk.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

| Payment Method                                                                 | Risk Rating |
|--------------------------------------------------------------------------------|-------------|
| Bank transfers (Klarna, Trustly, Rapid, ApplePay), debit cards issued by banks | Low         |
| EEA licensed e-wallets (Skrill, Neteller, paysafecard)                         | Medium      |
| Prepaid cards and vouchers                                                     | High        |

Manipulations with payment methods, such as using multiple accounts or inconsistent transaction patterns, are also flagged as high-risk activities.

Transactions involving cash and cryptocurrencies can carry elevated risks, primarily due to difficulties in tracing and validating the origins of funds and establishing clear customer identities. Given their potential use in concealing fund sources or identities, the Company may apply heightened scrutiny and additional enhanced due diligence (EDD) measures for customers utilizing these payment options.

### 3.2.5. Fraud red flags

The Company employs an anti-fraud risk management system designed to prevent bot attacks, fraudulent traffic, synthetic identities, account takeovers, identity theft, credit card and card-not-present (CNP) fraud, proxy users, multi-accounting, and more. Certain fraud indicators may also be linked to money laundering activities.

If the Company identifies that a player has triggered a fraud red flag, the player may be subjected to Enhanced Due Diligence (EDD).

## 3.3. Risk Score Calculation

The objective of this procedure is to detect minor instances of ML/FT behavior that, on their own, may not raise suspicion but could indicate risk when considered alongside other behaviors.

The internal CMS system will evaluate players based on several factors and assign a risk score. Each factor contributes to the overall score, with the total risk score being the sum of the individual scores. A higher negative score indicates a higher risk level.

| Indicator                | Description                               | Score |
|--------------------------|-------------------------------------------|-------|
| <b>Individual status</b> |                                           |       |
| PEP                      | A customer considered to be PEP           | 100   |
| Adverse media            | A customer was mentioned in negative news | 50    |

**Whitebox B.V.**  
**AML Policy and Procedures**

Version 4.1

|                                             |                                                                                                                                 |     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----|
|                                             | or information the company discovered from various sources                                                                      |     |
| Sanctions/blacklist                         | A customer is under international sanctions/blacklists                                                                          | 50  |
| <b>Geographical location</b>                |                                                                                                                                 |     |
| Not at home                                 | A customer whose IP location is different from their registered address                                                         | 20  |
| High-risk country resident                  | A customer resides in a High-risk country                                                                                       | 30  |
| <b>Gambling behaviour</b>                   |                                                                                                                                 |     |
| Large sums no play                          | A customer depositing large sums, then places minimal stake bets, then withdrawing all their funds                              | 50  |
| Large sums big losses                       | A customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence (EUR 5000 per week) | 50  |
| Low odds betting                            | A customer repeatedly placing short odds (such as red/black on roulette or repetitive betting on favourites) bets               | 25  |
| Big changes in money                        | Dramatic changes in terms of volume and size of player deposits or staking activity                                             | 20  |
| Several gaming accounts                     | A customer is trying to register several gaming accounts                                                                        | 30  |
| <b>Transactional behaviour</b>              |                                                                                                                                 |     |
| Smurfing                                    | A customer making multiple deposits or withdrawals of small amounts without no objective reasons                                | 30  |
| Spending above wages                        | A customers spend is outside of their affordability                                                                             | 20  |
| No withdrawals                              | Player has never requested a withdrawal                                                                                         | -20 |
| Withdrawal without playing                  | Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gambling            | 30  |
| <b>Payment methods the player is using</b>  |                                                                                                                                 |     |
| Card switching                              | A customer opening an account and registering several different cards and making transfers between them                         | 20  |
| High risk payment methods                   | A customer uses high-risk payment methods                                                                                       | 30  |
| <b>Fraud red flags a customer triggered</b> |                                                                                                                                 |     |
| VPN                                         | Customer used a VPN                                                                                                             | 30  |

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

Once the score is calculated, a risk level is assigned:

| <u>CMM Score</u> | <u>Risk Category</u> |
|------------------|----------------------|
| 0-20             | Low                  |
| 21 - 40          | Medium               |
| 41 - and higher  | High                 |

Due to technical and practical limitations, not all factors can be automatically included in the Customer Risk Assessment (CRA) calculation. However, we address these risks through other monitoring methods. For instance, we check for VPN usage and multi-accounting during registration, have separate alerts for players using cards under different names, and review all withdrawals before approval and payment.

### 3.4. Customer Due Diligence level

The level of customer due diligence (CDD) conducted on a player will depend on the risk score assigned to the player as follows:

|                                                          | Low | Med | High                   |
|----------------------------------------------------------|-----|-----|------------------------|
| Verify ID and address with docs                          | X   | X   | X                      |
| Collect additional personal details                      | X   | X   | X                      |
| Collect Source of Funds/ Wealth info                     |     | X   | X (with documentation) |
| Ongoing monitoring                                       | X   | X   | X (Enhanced)           |
| Additional measures to address any other risk identified |     |     | X                      |
| Report suspected cases of ML/FT                          | X   | X   | X                      |

The frequency of customer reviews depends on their assessed risk level, considering factors like geographic location, transaction behavior, and source of funds. Customers classified as high-risk—including those from higher-risk regions or exhibiting suspicious activities—are subject to more frequent monitoring. Medium-risk customers undergo regular periodic assessments, whereas low-risk customers have reviews performed less frequently. The Company regularly updates the frequency of these assessments in accordance with regulatory standards and revises them if significant changes in a customer's risk profile occur.

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

### **3.5. Additional Details & Source of Funds/Wealth**

As part of the customer risk assessment process, the Company considers the nature and consistency of a customer's income. A player having a single and regular source of income—such as a salary from lawful employment—generally presents a lower ML/TF risk. In contrast, customers with multiple, irregular, or unverifiable income streams may be classified as higher risk and subject to enhanced due diligence.

A daily report will be sent to the Compliance Officer, detailing any player who has been newly classified as medium or high risk, as well as any player whose risk level has escalated from medium to high.

The responsible AML manager will review all accounts in the report, including checking the information the Company already has on them, conducting open source internet checks, and assessing if there are any suspicious indicators. Based on these findings, the manager may take actions such as applying suitable Due Diligence measures, reviewing the responses and information provided by the player, or blocking the account if necessary.

Accounts classified as medium or high risk will require AML approval before any withdrawal requests can be processed.

All decisions taken by the AML manager must be documented.

### **3.6. On-Going Monitoring**

The AML team will conduct on-going monitoring on accounts, on a risk sensitive basis. This includes:

- Obtain fresh identification when existing documents have expired;
- Question the data and information about a player whenever inconsistencies are noticed;
- And in general review and update from time to time, on a risk sensitive basis.

### **3.7. Withdrawals**

When the AML Team review a withdrawal request, they will also look at the player's risk level:

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

- If the player has been classified as medium or high risk, the Verification Team will review the players documentation, and ensure that all the documents are still valid;
- If any documents have expired, new documents will be requested.

Therefore, any withdrawal request by a player who is flagged as medium or high risk, or any withdrawal request that has been otherwise flagged as high risk, will require approval by the AML team before being approved and processed.

## 4. Customer Due Diligence

### 4.1. Introduction

The Company differentiates between standard, simplified, and enhanced customer due diligence procedures. Customers are required to cooperate in fulfilling these due diligence obligations. If the Company is unable to perform the due diligence, the business relationship will not be established or continued, and no transactions will be processed. Additionally, the Company will evaluate whether it is necessary to submit an UTR.

### 4.2. Standard Customer Due Diligence

The Company implements standard customer due diligence (hereinafter – CDD) measures at the registration stage. The CDD process includes:

- **Identification:** Establishing the customer's identity by collecting relevant information.
- **Verification:** Confirming that the customer is who they claim to be by obtaining and validating documents or information from reliable and independent sources.
- **Beneficial owner:** Determining the identity of the beneficial owner and taking necessary measures to verify their identity, ensuring the casino fully understands who the beneficial owner is.
- Gaining an understanding of the **purpose and intended nature of the business relationship** and collecting additional information where required.

To meet these requirements and prevent money laundering and terrorist financing, the Company may collect the following information for identification and verification:

- a) Last name(s),
- b) First name(s),
- c) Date of birth,
- d) Address (street, no., ZIP code, city),
- e) Place of birth,
- f) Nationality

g) Identity number

### **4.3. Documents acceptance**

To verify a customer's identity, the Company requires a government-issued document containing photographic evidence of the customer's identity. The following documents are acceptable for this purpose:

- Current signed passport;
- Driving licence;
- Identity card;
- Travel document or passport.

For POA verification the Company accepts:

- Utility bill for a service installed at the residence issued in the last 3 months;
- Correspondence or any other government-issued document from a central or local government authority, department or agency issued in the last 3 months;
- Lease agreement (Does not have to be issued in the last 6 months but must be currently valid).

The key requirements for documents submitted by the customer are:

- The document must be current and not expired;
- Documents should be clear, easily readable, and of high quality;
- Mobile phone bills may not be accepted.

### **4.4. Threshold approach**

The Company applies CDD measures in relation to any transaction that amounts to EUR 2000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked, engage in occasional transactions exceeding this threshold, raise suspicions of money laundering or terrorist financing, or if the casino has doubts about the accuracy or completeness of previously collected customer identification information. If the EUR 2000 threshold is met and CDD is incomplete, the customer will be prevented from depositing or withdrawing funds. If the customer does not provide the required documentation when needed, the account will be closed after 30 days, and a report of unusual

## Whitebox B.V. AML Policy and Procedures

Version 4.1

activity will be filed if there is a reasonable suspicion.

A "transaction" includes both deposits and withdrawals of funds:

- **Deposits:** Funds added to an account for participating in remote gambling.
- **Withdrawals:** Funds taken out of an account, including:
  - Withdrawal of deposited funds used for gambling.
  - Collection of winnings from gambling activities.

Transactions are considered linked if they occur as part of the overall activity undertaken by a customer during a single session on the operator's gambling platform. However, this example is not exhaustive, and the Company considers other scenarios where transactions might be linked using a risk-based approach.

It is important to assess whether there are other circumstances in which transactions may also be considered linked, such as when a customer intentionally distributes their bets or winnings across multiple transactions to bypass CDD/EDD requirements or exhibits other suspicious behaviour.

For the purpose of the CDD triggered by the threshold, the Company applies verification using a risk-based approach.

The Company may also conduct Customer Due Diligence (CDD) at any time if there is a suspicion of money laundering or terrorist financing, or if the Company has doubts about the accuracy, reliability, or adequacy of previously obtained customer identification data.

### 4.5. Ongoing monitoring

The AML Team conducts ongoing monitoring of player accounts on a risk-sensitive basis, which includes:

- **Obtaining Fresh Identification:** Requesting updated identification documents when existing ones have expired to ensure all documentation remains current and valid.
- **Questioning Inconsistencies:** Reviewing and addressing any inconsistencies in the data and information provided by players.
- **Periodic Reviews:** Regularly reviewing and updating player information and documentation, particularly for those classified as

## Whitebox B.V. AML Policy and Procedures

Version 4.1

medium or high risk.

- **Transaction Matching:** Checking if transactions align with the documents and information available at the Company about the customer and the origin of the customer's assets.
- **Document and Data Updates:** Updating the respective documents, data, or information at appropriate intervals to ensure ongoing accuracy and relevance.

To ensure all customer information remains current, the Company conducts CDD procedures every six months following the initial successful verification of each customer, and additionally on a risk-sensitive basis.

### 4.6. Enhanced Due Diligence

#### Application of EDD Measures

The Company implements enhanced customer due diligence (EDD) measures and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the risks of money laundering and terrorist financing.

#### Instances Requiring EDD

- When identified by the Company or indicated by authorities as a high risk for money laundering or terrorist financing;
- When there are doubts about the accuracy or validity of the customer's identity information;
- When it is discovered that a customer has provided false or stolen identification documents or information, and the Company decides to continue the relationship;
- When transactions are complex or unusually large, exhibit unusual patterns, or lack apparent economic or legal purposes;
- When a customer's winnings are paid to a different account than the one used for wagers;
- Any other scenario that presents a higher risk of money laundering or terrorist financing.

In high-risk cases, establishing or continuing a business relationship requires the consent of the Compliance Officer.

#### EDD Procedures for High-Risk Customers

## Whitebox B.V. AML Policy and Procedures

Version 4.1

For customers deemed high-risk or becoming high-risk, the Company undertakes EDD measures, which may include:

- Re-verifying the customer's identity (repeated CDD);
- Establishing the legitimacy of the customer's wealth through documentation such as:
  - Salary income or company profit (payslips, employer letters, or audited accounts);
  - Sale or liquidation of financial instruments (Certified sale contracts or statements, accountant letter, etc.);
  - Sale of property (Certified copy of sale contract, letter from solicitor or estate agent);
  - Inheritance (Certified copy of will including the value of inheritance);
  - Sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor);
- Confirming that the source of the customer's funds does not originate from criminal activities;
- Ensuring deposits come from identifiable payment methods by requesting bank or account statements;
- Conducting increased continuous monitoring of the business relationship;
- Investigating suspicious transactions and monitoring the underlying business relationship to assess money laundering and terrorist financing risks.

The primary aim of EDD on transactions is to ensure the transparency of payment flows. Each transaction's origin and destination must be traceable back to an account.

### Definitions

**Source of Funds:** Refers to the origin of the specific funds used for deposits on the Company's website. This involves verifying more than just the bank or financial institution; it requires substantive information that establishes the funds' origin and acquisition method.

**Source of Wealth:** Refers to the origin of the customer's total assets. The Company must obtain information indicating the volume of wealth reasonably expected for the client and providing a clear picture of how this

wealth was acquired.

#### **4.7. Politically Exposed Persons and Sanctions Screening**

The Company employs KYC software to screen all new customers during registration or during an occasional transaction against PEP and Sanctions databases. In addition, if a customer's total deposits or transactions exceed €2,000 within any 30-day period, a PEP check is triggered immediately. This service also performs regular checks on the entire customer database every six months to ensure that the status of existing customers has not changed.

Any new or existing customer found in the Sanctions database, identified as a PEP, or related to a PEP will have their account rejected or closed.

When a PEP is identified, responsible staff will report to the Compliance Officer, who will then inform senior management.

The Compliance Officer will investigate each case to determine whether the PEP alert is a positive or false-positive match. The Company reserves the right to request additional documents from the customer during the investigation.

If the PEP alert is confirmed, the Compliance Officer will reject the registration or close the account and notify senior management of the decision.

#### **Definition of Politically Exposed Person (PEP)**

A PEP is an individual entrusted with a prominent public function at the international, European, or national level, or with a public position of comparable importance below the national level. Specifically, PEPs include:

- Heads of state, heads of government, ministers, members of the European Commission, deputy ministers, and assistant ministers.
- Members of parliament and similar legislative bodies.
- Members of governing bodies of political parties.
- Members of supreme courts, constitutional courts, or other high-level judicial bodies whose decisions are typically not subject to appeal.
- Members of boards of courts of audit.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- Members of boards of central banks.
- Ambassadors, chargés d'affaires, and defence attachés.
- Members of administrative, management, or supervisory bodies of state-owned enterprises.
- Directors, deputy directors, board members, or other managers in international or European intergovernmental organizations.

### Definition of PEP Family Member

A family member of a PEP includes close relatives, specifically:

- The spouse or civil partner.
- A child and the child's spouse or civil partner.
- Both parents.

### Sanction Lists Adhered to by the Company

The Company adheres to the following sanction lists:

- Consolidated United Nations Security Council Sanctions List
- Consolidated list of persons, groups, and entities subject to EU financial sanctions
- OFAC (Office of Foreign Assets Control) Sanctions List
- HMT (Her Majesty's Treasury) Sanctions List
- Sanction Decree "Al-Qaida" (N.G. 2015, no. 29)
- Ministerial Regulation "Libya" (N.G. 2015, 28)
- Sanction Decree "Islamic Republic Iran 2015" (N.G. 2015, 27)
- Sanction Decree "Democratic People's Republic of Korea 2015" (N.G. 2015, 30)
- Ministerial Regulation "Yemen" (N.G. 2015, 65)

All funds or assets belonging to sanctioned individuals must be immediately frozen, and a corresponding report must be promptly submitted to the relevant authority.

### FATF Blacklisted/Grey-listed Countries

The Company blocks individuals from FATF blacklisted and grey-listed countries from registering or logging into its sites. The list of these countries can be found here: <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

**Whitebox B.V.**  
**AML Policy and Procedures****Version 4.1****4.8. Procedure for Account Closure**

The Company may decide to close a customer's account for various reasons, including:

- Fraud
- Cheating
- Bonus abuse
- Allowing third-party use of the account
- Collusion
- Under-aged gambling
- Problem gambling
- Abusive behavior towards staff
- Commercial concerns
- Failure in Customer Due Diligence (CDD)
- Breach of Terms and Conditions

The primary concern addressed by this Company Policy is when there is suspicion or knowledge of the customer being involved in money laundering (ML) or terrorist financing (TF).

**Legal Obligations and Account Closure**

By law, the Company must terminate the business relationship with a customer if there are ML/TF concerns unless appropriate consent to continue the relationship has been obtained. Even with consent, it is often prudent to close the account as a precaution.

Due to anti-tipping off regulations, the Company cannot inform the customer about the specific ML/TF concerns. Therefore, account closure must be handled discreetly.

**Compliance Officer's Role**

The Compliance Officer must evaluate whether an Unusual Transaction Report (UTR) has been submitted related to the customer's behavior and whether appropriate consent for continuing the relationship should have been requested.

If the Company cannot complete or apply the required CDD measures when the CDD threshold for transactions is reached, it is legally obligated to cease transactions and terminate the business relationship with the customer.

## **5. Deposit and Withdrawal Management Procedures**

### **5.1. Player Account Balance**

Each player has a wallet where funds are managed, with bets deducted and winnings added. All funds deposited by the player or owed by the Company are credited to the player's account. Players can add funds to their accounts by depositing through the site's cashier and then use these funds to place bets. Bets are deducted from the account balance, and winnings are added to it.

Players can withdraw available funds from their account balance. The Company does not offer credit to players, and funds may not be transferred between players.

### **5.2. Payment Methods**

Payments are only accepted and made from accounts held with licensed financial institutions or through licensed payment providers. The Company reserves the right to restrict the use of certain payment methods from specific countries based on risk assessments and regulatory requirements.

No cash deposits or withdrawals are permitted between the Company and its players.

### **5.3. Player Deposits**

After registering, players can deposit funds into their accounts through the site's cashier.

To facilitate these deposits, the Company has integrated with several gateways, all of which are PCI DSS compliant. The Company does not store any credit card data.

The Company submits the transaction to the payment service provider (PSP) and waits for approval from the card acquirer or e-wallet. Once approved, the deposit status is updated, and the funds are added to the player's balance.

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

## **5.4. Player Withdrawals**

Players with an available balance can request a withdrawal through the site's cashier.

Players will specify the amount they wish to withdraw and select their preferred payout method. The requested amount is then deducted from the player's balance.

## **5.5. Withdrawal Payouts**

When remitting funds to the player, we will, whenever possible, transfer the funds directly to the account from which they originated. If this is not possible, we will remit the funds to the player in accordance with AML legislation requirements.

## **5.6. Verification and Conditions**

The Company enforces measures to ensure that all deposits and withdrawals align with the customer's registered account information.

**Verification of Cardholder's Name:** The name on the payment method, whether a card or bank account, must match the name registered on the player's account. Any discrepancies will trigger a review process, during which the Company may request additional documentation or suspend transactions until verification is complete.

**Handling of Inconsistencies:** If inconsistencies are identified between the player's account details and the payment method, the Company reserves the right to conduct further checks. This ensures the legitimacy of the payment method and its proper association with the player.

**Minimum Wagering Activity:** To prevent the abuse of bonuses or promotional offers, the Company may impose minimum wagering activity requirements before processing withdrawals.

## 6. Suspicious and Unusual Activity Reporting

### 6.1. Introduction

All employees have an obligation to promptly report to the Compliance Officer any unusual or suspicious transactions, as well as any knowledge or suspicion of money laundering (ML), terrorist financing (TF), or proliferation financing (PF) derived from player activity on the Company's platform.

The Compliance Officer will evaluate each report to determine whether there are reasonable grounds for reporting. If such grounds exist, a formal **Unusual Transaction Report (UTR)** will be electronically submitted to the Financial Intelligence Unit (FIU) Curaçao.

**Knowledge:** The reporting individual possesses direct evidence or knows the illicit event/origin to be a factual certainty.

**Suspicion / Unusual Behavior:** The reporting individual notices activity that deviates from normal player typologies, fails to make commercial or financial sense, or matches established regulatory red flags.

A transaction may not initially appear unusual, but if concerns or patterns arise later, the obligation to report is triggered immediately upon retroactively identifying the anomaly.

### 6.2. Red Flags Indicators

Red flags are indicators that may prompt the Company to question a customer's behavior but do not automatically result in a UTR being filed with the FIU, but they legally mandate an internal escalation to the Compliance Officer.

**Possible red flags include:**

- A customer not cooperating with CDD/EDD.
- A customer attempting to register multiple accounts on a site.
- A customer making small wagers despite significant deposits, followed by a large withdrawal request.
- Frequent deposits and withdrawal requests without reasonable explanation.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- Significant changes in a customer's gaming patterns.
- A customer inquiring about moving funds between accounts within the same gaming group.
- Transactions disproportionate to the known wealth, income, or financial situation of the customer.
- A customer seeking to transfer funds to a third-party bank account.
- Withdrawal requests to an account not previously used for deposits.
- A customer registering multiple cards and transferring funds between them.
- Large deposits followed by minimal betting and large withdrawals.
- Large losses without apparent concern.

### 6.3. Inability to Complete CDD Measures

If a customer refuses to provide mandatory CDD/EDD documentation, or provides intentionally evasive answers, the Company **cannot** establish or maintain the business relationship. The account must be immediately restricted, and the company will assess all surrounding factors—including payment methods, games played, and geolocation. If grounds exist to suspect the funds are tied to illicit activity, an internal report must be routed to the Compliance Officer for UTR evaluation.

### 6.4. Internal Unusual Transaction Report (Internal UTR)

All employees are required to report unusual transactions or behaviors to the Compliance Officer immediately using the **Internal Unusual Transaction Report Form**. Employees must submit these reports even if their operational superiors or commercial managers disagree. The Compliance Officer maintains independent veto power regarding compliance files.

**An Internal UTR should include:**

- Customer details (User ID, full name, registering details).
- The employee's statement explaining the cause for the report.
- All relevant documentation and information.

**The Compliance Officer will:**

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- Acknowledge receipt of the report and conduct further investigation as required.
- Conduct a deeper secondary forensic financial investigation into the player's account history.
- Determine whether the data satisfies the objective or subjective indicators established by FIU Curaçao.
- Maintain a centralized, secure log of the decision-making process, regardless of whether an external report is ultimately filed.

### 6.5. External report to FIU

Upon receiving an Internal UTR, the Compliance Officer will determine if an external notification is legally required. When making this decision, the Compliance Officer must consider that AML/CFT/CPF legislation is designed to detect and deter the abuse of the financial system for criminal purposes.

While isolated technical matters like simple identity fraud or commercial chargebacks may not automatically represent systemic laundering, they will trigger external reporting if they show an intent to obscure the origin of funds or form part of a coordinated scheme.

When deciding whether to submit a UTR to the authorities, the Compliance Officer must answer the following operational questions:

[Who is involved?] —> [How are they executing transactions?] —> [What is the value of the assets?] | [Why is the activity deemed unusual?] <—  
[When & where did it arise?] <—

### 6.6. Reporting Procedure via goAML

The Company is strictly obliged to submit an external Unusual Transaction Report (UTR) to the authorities **without due delay** the moment the Compliance Officer determines an objective or subjective indicator has been met.

- **Mandatory Digital Portal:** All submissions must be transmitted securely and electronically through the **goAML portal**, the specialized interface managed exclusively by **FIU Curaçao**. Submission via physical mail or unencrypted email is strictly prohibited.
- **Strict Prohibitions:** The Company does not execute or process transactions known or heavily suspected to be linked to financial crime, except in rare circumstances where delaying the transaction

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

is technically impossible or would directly hinder the prosecution of an ongoing law enforcement investigation.

### **6.7. Tipping-off**

It is an offence to tell anyone that an UTR has been submitted or is being considered to be submitted and that this is likely to prejudice the investigation. This means it is possible to have an internal discussion about the customer, but in no way can the customer or their associates be given any indication that the customer may be under investigation.

This means that no one working for the Company:

- Can, at the time, tell a customer that a transaction is being delayed because a report is awaiting a defence (consent) from the FIU;
- Can tell the customer that law enforcement is conducting an investigation.

## **7. Internal Control**

### **7.1. Introduction**

The Company has implemented various internal controls and general procedures that are utilized daily to manage and operate the business, specifically aimed at preventing money laundering and terrorist financing.

### **7.2. Employees background check**

Before hiring employees, the Company will conduct thorough integrity checks appropriate to the candidate's position, responsibilities, and access levels. The Company will not employ individuals who are not considered fit and proper.

Once employed, ongoing screening of employees will be performed as required. All employees must comply with applicable legislation and due diligence obligations, report any facts relevant to money laundering, and avoid participating in dubious transactions, whether actively or passively.

To ensure compliance, senior management will conduct regular checks on employees and additional inspections as needed. These checks will be particularly stringent when there is suspicion regarding the behavior of specific employees. The Company may conduct these inspections through surprise spot checks or other methods to verify adherence to policies and procedures.

The frequency and extent of screening will be proportionate to the risk level posed by the employee, which will be determined on a case-by-case basis, considering the employee's position (e.g., head of department, senior, mid-level), scope of duties, and responsibilities.

The Company will conduct background checks on all employees at least once a year, using an employee performance sheet for this purpose.

### **7.3. Record keeping**

The Company maintains all documents and data collected or obtained during due diligence, including:

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- All data and information used to identify and verify customers (such as type and number of the document, issuing authority, etc.).
- All transaction records (receipts) related to winnings paid out or refunds to customer accounts.
- All documents and records used for the preparation of the risk analysis, the risk analysis itself, including the results of the risk assessment, and documentation on the appropriateness of the measures taken based on these results.
- Results of internal investigations and communications with the FIU and regulators.
- Documents collected during due diligence of business partners.
- Documents collected from employees during due diligence.
- Documents related to AML training (training materials, examination results, etc.).

The Company also retains all documents created and processed in connection with suspected money laundering or terrorist financing, including:

- All related internal and external correspondence.
- File and interview notes.
- Results of internal investigations and measures taken, explaining why the money laundering officer concluded and initiated the actions.

The retention period is five years, starting at the end of the calendar year in which the business relationship ends, or in all other cases, at the end of the calendar year in which the respective information was obtained. Applicable legislation may provide for a longer retention period.

After the expiration of the retention period, the Company destroys all collected documents and data unless other recordkeeping or retention obligations apply, but no later than 10 years.

### 7.4. Money Laundering Reporting Officer

The Company has appointed a Compliance Officer responsible for reviewing internal reports on unusual or suspicious transactions. When necessary, the Compliance Officer will submit an UTR to the FIU. This officer also acts as the primary point of contact for the FIU.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

To ensure the Compliance Officer can effectively perform their duties, the Company guarantees that:

- The Compliance Officer operates independently, possesses thorough knowledge of the Company's activities, and can autonomously decide whether to escalate internal reports to the FIU.
- There are no conflicting responsibilities that could create a conflict of interest.
- The Compliance Officer has sufficient time, resources, and information to carry out their responsibilities.
- The Compliance Officer has the authority to assign tasks to relevant employees and make decisions regarding ML and TF prevention.

The Compliance Officer and their deputy perform the following functions, among others:

- Developing and continuously refining internal risk assessments covering all ML and TF risks.
- Creating and updating internal policies and procedures aimed at preventing ML and TF.
- Establishing clear and consistent reporting channels.
- Participating in the development and implementation of other internal organizational guidelines related to AML and CTF regulations.
- Ensuring the Company's operations comply with current AML regulations and relevant legislation.
- Monitoring business activities to ensure adherence to money laundering regulations.
- Ensuring proper execution of CDD and EDD procedures.
- Evaluating the risk associated with suspicious activities.
- Filing UTRs when necessary.
- Contributing to the development of AML training content for staff.
- Keeping records of all inquiries from law enforcement and maintaining documentation related to internal and external disclosures.
- Reporting to senior management on the Compliance Officer's activities, the Company's risk profile, and the measures taken to comply with money laundering regulations.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

The Compliance Officer and their deputy are authorized to:

- Perform their duties independently and effectively.
- Issue legally binding statements on behalf of the Company and represent it in relevant external matters.
- Provide directives specific to the Company regarding AML and CTF prevention.
- Conduct unrestricted random checks to ensure compliance.

### 7.5. Training

The Company will provide training to all staff, either directly or through a service provider, upon their joining and annually thereafter.

Training materials tailored to each team will be prepared in alignment with Company policies, which are based on applicable legislation and guidelines.

#### Training Implementation

- Training materials will be derived from finalized and approved Company policies, delivered through documents and presentations.
- Existing management and staff will receive training in classroom settings or online.
- New staff will undergo training as part of their induction process.
- Post-training, a questionnaire will assess the staff's understanding.
- If issues are identified, additional training sessions will be conducted to address any unclear areas.
- Regular refresher training will be provided, incorporating updates and addressing any shortcomings observed during the previous period.
- Policy updates will be communicated via group emails, ad-hoc training sessions, and included in periodic training updates and materials.

#### Training Focus Areas

Training will ensure staff awareness of:

- Relevant legislation.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- Requirements for preventing money laundering and terrorist financing.
- Personal obligations under these requirements.
- Internal reporting procedures.
- Company policies and procedures to combat money laundering and terrorist financing.
- Identification, verification, record-keeping, and other related procedures.
- Recognition and handling of suspicious transactions.
- Personal liability for failing to report information or suspicions.
- Current techniques, methods, and trends in money laundering and terrorist financing.
- The specific ML and TF risks faced by the Company.
- Data protection regulations.

### Induction and Refresher Training

Induction training sessions for all new employees will cover fraud prevention, detection, and related topics relevant to their roles. Refresher training will be provided regularly and as needed to keep employees updated on Company policies, procedures, and any changes or improvements made.

### Record Keeping

The Money Laundering Officer will maintain records of all training sessions, including the content provided, the dates, the trainers, and the next scheduled training. Any changes to Company policies, procedures, or applicable legislation will prompt relevant training for all staff.

## 7.6. Internal revision and staying up to date

The Company has developed its policies and procedures in compliance with applicable legislation and guidance from the FATF, CGA, and FIU. However, these requirements and guidance, along with external fraud trends, are subject to change. To ensure that the Company's internal AML documentation remains current and relevant, the following measures have been implemented:

- Key personnel are subscribed to mailing lists from the FIU, CGA, and FATF, and participate in relevant forums.

## Whitebox B.V. AML Policy and Procedures

Version 4.1

- The Company regularly consults with gambling industry experts for advice on AML best practices.
- Upon receiving updates, the Company will take the following actions as necessary:
  - Revise Company policy documentation and training materials.
  - Notify all relevant staff via email about the updates, hold meetings with team managers, and ensure they brief their teams accordingly.
  - Update email templates and chat canned responses.
  - Refresh website policies, including version numbers and 'last update' dates.
  - Amend the Terms and Conditions, also including version numbers and 'last update' dates.

Any update to the Terms and Conditions will prompt a pop-up notification to players upon their next login, requiring them to accept and agree to the new version before proceeding.

The Company may appoint an independent third-party provider specializing in AML compliance to perform external reviews of the Company's AML policies and procedures. Outcomes from these reviews will be communicated to senior management and utilized to improve and refine AML/CTF processes and documentation where necessary. The senior management shall determine the frequency of such external reviews, which may occur annually or at shorter intervals based on the necessity to reassess and validate the effectiveness of the Company's AML program.

## **8. Compliance and Consequences of Non-Compliance**

The Entity is committed to full compliance with all applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) laws and regulations of Curaçao, including the National Ordinance on the Identification of Clients when Rendering Services (NOIS) and the National Ordinance on the Reporting of Unusual Transactions (NORUT), as well as any applicable guidance issued by the Curaçao Gaming Authority (CGA) and the Financial Intelligence Unit (FIU Curaçao).

All employees, officers, and relevant personnel are required to strictly comply with the obligations set out in this Policy and applicable legislation. These obligations include, but are not limited to, performing appropriate customer due diligence, monitoring customer activity, promptly reporting unusual or suspicious transactions to the FIU Curaçao through the prescribed reporting channels, maintaining confidentiality of reporting activities, and cooperating with competent authorities where required.

Failure to comply with AML/CTF requirements may expose the Entity and its personnel to significant regulatory, legal, financial, and reputational risks. Non-compliance may result in supervisory measures imposed by competent authorities, including administrative sanctions, financial penalties, operational restrictions, or other enforcement actions, in accordance with applicable laws and regulations.

In addition to regulatory consequences, any employee or officer found to be in breach of this Policy may be subject to internal disciplinary action. Such actions may include written warnings, suspension of duties, reassignment, termination of employment or contractual engagement, or other appropriate measures depending on the nature and severity of the violation.

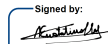
Serious or intentional violations of AML/CTF obligations may also result in criminal liability under applicable law. The Entity treats any instance of non-compliance with the utmost seriousness and may initiate internal investigations where breaches are suspected.

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

The Entity continuously monitors regulatory developments and periodically reviews and updates its AML/CTF policies and procedures to ensure ongoing compliance with the requirements of the FIU Curaçao, Curaçao Gaming Authority (CGA), and other relevant authorities.

Approved:

Signed by:  
  
8737E2B30CF043F...

Signed by:  
  
E9C14AA3F74E4ED...

Analissa HeilandLorenza Godett

Executive Corporate Management B.V.

Date: 20.05.2026

# **APPENDIX 1**

## **«COUNTRIES AND TERRITORIES EXCLUDED FROM REGISTRATION»**

**Whitebox B.V.**  
**AML Policy and Procedures****Version 4.1**

The following list includes countries subject to restrictions. Please note that this list is not exhaustive and may also encompass other countries banned for various reasons, such as changes in FATF recommendations, restrictions due to license agreements, or other deficiencies. The Company does not provide services to clients from the countries listed below.

1. Afghanistan
2. American Samoa
3. Aruba
4. Australia
5. Belgium
6. Belize
7. Bonaire
8. Bosnia and Herzegovina
9. Burma/Myanmar
10. Burundi
11. Central African Republic
12. Curaçao
13. Democratic People's Republic of Korea
14. Democratic Republic of the Congo
15. Denmark
16. Egypt
17. Eritrea
18. Estonia
19. France
20. French Guyana
21. Greece
22. Greenland
23. Guadeloupe
24. Guam
25. Holy See (Vatican City)
26. Iran (human rights)
27. Iraq
28. Italy
29. Ivory Coast
30. Kuwait
31. Lebanon
32. Libya
33. Lithuania
34. Malaysia
35. Maldives
36. Mali
37. Marshall Islands

**Whitebox B.V.**  
**AML Policy and Procedures**

**Version 4.1**

- 38. Martinique (.FR)
- 39. Netherlands
- 40. Occupied Palestinian Territory
- 41. Puerto Rico
- 42. Qatar
- 43. Russian Federation
- 44. Somalia
- 45. South Sudan
- 46. Sudan
- 47. Syria
- 48. USA
- 49. US Minor Outlying Islands
- 50. US Virgin Islands
- 51. Yemen
- 52. Zimbabwe