

BONUS Operations N.V.
(and Ozias Holding Limited)
AML/CFT Policy

This is a confidential document for Bonus Operations N.V. It contains confidential and/or proprietary information that may not be disclosed or discussed with anyone outside the organization without written approval of Bonus Operations N.V.

Table of Contents

1. Overview.....	5
1.1. Introduction	5
1.2. Management.....	5
1.3. Legal framework.....	6
1.4. Definitions	6
1.5. Data processing system	7
2. Customer Acceptance and Registration Policy	8
2.1. Purpose & scope.....	8
2.2. Customer Acceptance	8
2.3. Restrictions	8
2.4. Information Entered on Registration	9
2.5. Terms Acceptance	10
2.6. Underage Customers	10
2.7. Customer Due Diligence.....	10
3. Customer Risk Scoring and Profiling	11
3.1. Purpose & scope.....	11
3.2. Risk-based approach.....	11
3.3. Customer Risk Assessment.....	12
3.3.1. Individual status.....	12
3.3.2. Geographical location	13
3.3.3. Gambling and transactional behaviour.....	13
3.3.4. Payment Methods	14
3.3.5. Fraud red flags	14
3.4. Risk Score Calculation	14
3.5. Customer Due Diligence level.....	15
3.6. Additional Details & Source of Funds/Wealth	16
3.7. On-going Monitoring	16
3.8. Withdrawals.....	17
4. Customer Due Diligence	18
4.1. Purpose & scope.....	18
4.2. Standard Customer Due Diligence	18
4.3. Documents acceptance	19

4.4.	Threshold approach.....	19
4.5.	Ongoing monitoring.....	20
4.6.	Enhanced Due Diligence.....	20
4.7.	Politically Exposed Persons and Sanctions Screening	22
4.8.	Procedure for Account Closure.....	24
4.9.	Corporate Customers (B2B).....	25
5.	<i>Funds Management Procedures.....</i>	26
5.1.	Player Account Balance.....	26
5.2.	Payment Methods	26
5.3.	Player Deposits.....	26
5.4.	Player Withdrawals	26
5.5.	Withdrawal Payouts	26
6.	<i>Crypto payments</i>	27
6.1.	Compliance with regulatory requirements	27
6.2.	Risks with crypto payments	27
6.3.	Unhosted wallets.....	28
6.4.	Custodial wallet services.....	28
6.5.	Volatility of VFAs	28
7.	<i>Suspicious Activity Reporting</i>	29
7.1.	Purpose & scope.....	29
7.2.	Red Flags / Indicators	29
7.3.	Inability to Complete CDD Measures	30
7.4.	Internal Suspicious Activity Report.....	30
7.5.	External report to FIU	31
7.6.	Reporting Procedure.....	32
7.7.	Tipping-off	33
8.	<i>Internal Controls.....</i>	34
8.1.	Purpose & scope.....	34
8.2.	Recordkeeping	34
8.3.	Money Laundering Reporting Officer.....	35
8.4.	Training.....	36
8.5.	Employees background check	38
8.6.	Internal and external revision and staying up to date	39
8.7.	Version Control	40

Disclaimer

NO PART OF THIS DOCUMENT MAY BE REPRODUCED, TRANSMITTED OR IN ANY OTHER WAY DISTRIBUTED WITHOUT THE PRIOR WRITTEN PERMISSION OF BONUS OPERATIONS N.V. ALL TECHNOLOGIES, DESIGNS, IMPLEMENTATIONS, TRADE SECRETS AND BUSINESS MODELS DESCRIBED HEREIN IS THE INTELLECTUAL PROPERTY OF BONUS OPERATIONS N.V. AND/OR IT'S PARTNERS AND IS PROVIDED FOR INFORMATION PURPOSES ONLY.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY CONCERNING ITS ACCURACY OR QUALITY. IN NO EVENT WILL BONUS OPERATIONS N.V. BE LIABLE FOR DIRECT OR INDIRECT DAMAGES RESULTING FROM INCIDENTAL DEFECTS OR INACCURACIES IN THIS DOCUMENT.

BONUS OPERATIONS N.V. RESERVE THE RIGHT TO REVIEW AND MODIFY DIGITAL COPIES OF THIS DOCUMENT AT ANY TIME WITHOUT PRIOR NOTICE.

1. Overview

1.1. Introduction

Bonus Operations N.V., a limited liability company incorporated under the laws of Curaçao, with the company registration number **161022**, having registered office Chuchubiweg 17, Willemstad, Curaçao (hereinafter – the Company).

The provisions in this Anti-Money Laundering Policy (this “Policy”) aim to reduce the possibility for the business of providing services by Bonus Operations N.V. to be used for criminal purposes or in violation of regulations.

Being a remote gaming entity authorized under Curaçao jurisdiction, Bonus Operations N.V. is deemed to be carrying out “relevant financial business” in terms of the GCB’s AML/CFT/CFP Regulations and thus Bonus Operations N.V. is a subject-person in terms of said Regulations. As such, it is required to abide by the applicable legislation and guidance relating to the prevention of money laundering and funding of terrorism.

This Policy provides guidance detailing responsibility regarding the prevention of money laundering and funding of terrorism from the perspective of the legal framework of Curaçao and internationally accepted regulations in this area. This information includes due diligence, monitoring, training and record-keeping policies and procedures, as well as a description of the role and responsibilities of the Key Compliance Officer.

1.2. Management

The Company has appointed a Key Compliance Officer as part of the art. 5g of the NOIS.

This policy applies to all employees and outsourced staff undertaking anti-money laundering, responsible gambling and anti-fraud procedures to the extent connected to their direct responsibilities, including Senior Management and the Key Compliance Officer.

The Key Compliance Officer is the key individual responsible for the prevention of money laundering and the financing of terrorism. He/she has overall responsibility for ongoing regulatory compliance and creating anti-money laundering procedures.

The Key Compliance Officer will be fully engaged in defining and managing the processes needed to prevent money laundering and other fraudulent activity based on the following principles:

- The Company assumes that most customers are not money launderers. However, it identifies players since it requires the applicable regulations, using a risk-based approach.
- The Company monitors all transactions and activity.

- The Company continuously monitors its customers, as well as risks and processes.

The Company will ensure that all relevant employees are trained on AML and CTF policies and procedures and emphasize alerting these risks. Relevant employees will be required to pass competency tests on this topic.

1.3. Legal framework

The Company's AML Policy and all related procedures were created subject to the relevant applicable legislation, in particular (but not limited to):

- Curaçao - National Ordinance Reporting Unusual Transactions (NORUT);
- National Ordinance Identification when Rendering Services (NOIS);
- National Ordinance Penalization of Money Laundering (NOPML);
- EU-Directive 2015/849 of the European Parliament and of the Council;
- EU-Directive 2018/843 of the European Parliament and of the Council;
- EU-Directive 2018/1673 Of the European Parliament And Of The Council;
- The FATF Recommendations.

1.4. Definitions

Money laundering is the process of concealing, disguising, converting, transferring, or removing criminal property. In other words, it is the process of converting the proceeds of crime into assets with legal origin.

There are three stages of money laundering:

1. **Placement** – placement of funds generated from crime into financial system, either directly or indirectly (blending of funds, invoice fraud, smurfing).
2. **Layering** – the process of separating illicit proceeds from their source by creating complex “layers” of financial transaction designed to disguise the audit trail and provide anonymity (multiple bank transfers, investing in “cash” business).
3. **Integration** – the provision of apparent legitimacy to criminal derived wealth. 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 and appear to be legitimately earned or acquired funds (property dealing).

Terrorist financing is the provision or collection of funds with the intention that they should be used (or in the knowledge that they are to be used) to carry out acts that support terrorists or terrorist organizations or to commit acts of terrorism.

The key differences between ML and TF are:

- For money laundering to occur, the funds involved must be the proceeds of criminal conduct.
- For terrorist financing to occur, the source of funds is irrelevant, i.e., the funds can be from a legitimate or illegitimate source.

However, they both involve money or other forms of value. They both involve the movement of money or value, for example, from one person to another, one account to another, one institution to another, one country to another, one asset class to another. They are both keen to disguise the source and destination of funds.

Bonus Operations N.V. developed internal security measures to prevent money laundering and terrorist financing. The key features of these measures aim to stay aware of high-risk customers and detect suspicious activity, including the predicate offenses to money laundering and terrorist financing.

1.5. Data processing system

The Company operates its internal data processing system to detect high-risk scenarios, money laundering, and terrorist financing in day-to-day operations.

The Data processing system consist of the following mechanisms:

- identification of all users upon the business relationship is established;
- Politically Exposed Persons (PEP) and sanction list checks are performed by the relevant software;
- transaction monitoring is managed by trained staff;
- reporting of all suspected money laundering cases to the Key Compliance Officer and the Curaçao FIU.

The Company will monitor trends and changes connected to ML/TF and will develop additional internal procedures to keep it up to date.

2. Customer Acceptance and Registration Policy

2.1. Purpose & scope

Before making a deposit or place real-money stakes, the customer must register a gaming account. Customers who do not register an account will not be able to play on the Company's website.

In case of Corporate Customers (B2B), additional checks will be conducted including background checks and full corporate due diligence.

The Customer Acceptance and Registration Policy defines the criteria by which the Company may or may not accept potential customers and describes the registration process.

2.2. Customer Acceptance

In order to deposit and play on the Company's website, a customer must first register on the site.

Registration is limited to individuals who are over eighteen (18) years of age.

Customers may only open one account in their name per site. Additional checks are run to block multiple accounts by email address, mobile number, device and certain other combinations of customer data. These checks are done in order to prevent customers opening multiple accounts in order to bypass the AML threshold.

Corporate customers, willing to resell the company's product, must provide the Company with extra due diligence which will be reviewed directly by the appointed 'day-to-day' AML officer. Requirements are implemented directly by the Company's management and appointed Money Launder Reporting Officer, who oversees operations at corporate level.

Each corporate customer must be approved by the appointed day-to-day AML officer before the company can enter any business relationship with him/her. Due Diligence must be stored separately to those of standard (B2C) customers and needs to be easily accessible for the Company's Money Laundering Reporting Officer. Specific requirements for corporate customers can be found in Clause 4 of this AML policy.

2.3. Restrictions

- Individuals under 18 years of age are not permitted to register on the site.
- Individuals considered to be PEP, under Sanctions or listed in any blacklists, in particular: the Consolidated United Nations Security Council Sanctions List¹², the Sanction Decree "Al-Qaida c.s., the Taliban of Afghanistan c.s., ISIL c.s., ANF c.s." (N.G. 2015, no. 29), the

Ministerial Regulation “Libya” (N.G. 2015, 28), the Sanction Decree “Islamic Republic Iran 2015” (N.G. 2015, 27);, the Sanction Decree “Democratic People’s Republic of Korea 2015” (N.G. 2015, 30), and the Ministerial Regulation “Yemen” (N.G. 2015, 65).

- Existing customers who have an existing exclusion on the site.
- Individuals with fraud red flags.
- Entities flagged by regulatory bodies.
- Entities directly or indirectly owned by any PEP.
- Entities listed on an active sanctions list.

Corporate entities may get rejected at the discretion of the AML Officer, MLRO or Senior Management if the company feels that the client does not implement sufficient AML practices.

If the AML Officer finds anything suspicious upon reviewing of the new corporate customer, they should report this immediately to the MLRO and the Senior Management. Jointly they will make a decision if the corporate customer can get accepted and if not, the MLRO should decide to file a SAR to the Local authorities with their findings regarding this rejected customer.

2.4. Information Entered on Registration

During the registration process and later on, the Company will request the following identifying information and contact details:

- First Name and Last Name,
- Date of Birth,
- Gender,
- Residential address and country of Residence,
- Email address and mobile phone number,
- Username and Password.

2.5. Terms Acceptance

During the registration process, the customer must also confirm acceptance of the website's general terms & conditions and its privacy policy.

2.6. Underage Customers

The system does not allow registration of customers who are underage. In order for the registration process to be successful, customers must be at least 18 years old or of legal age in their territory. Date of Birth will be cross checked with the provided ID upon Customer Due Diligence check.

2.7. Customer Due Diligence

To complete registration the customer must identify his/her personal data such as first name, last name, residential address, date of birth, email address, phone number. If the identification is failed at any point, the registration will be declined. Upon customer's first withdrawal attempt the Company requests documents (such as ID, Proof of Address) in order to verify the identity of the player.

3. Customer Risk Scoring and Profiling

3.1. Purpose & scope

Within the risk-based framework, the Company will undertake risk profiling of all customers from the time of registration for potential money laundering/terrorism financing risks.

It is important to note that the Company's policies and procedures are based on the following:

- Actual regulatory and legal requirements;
- Guidance provided by GCB and Curaçao FIU;
- Internal evaluation of the Company's business risk assessment, and knowledge and experience about the customers.

3.2. Risk-based approach

The Company undertakes a risk-based approach to prevent and combat money laundering and terrorist financing. The Company's risk-based approach is covering the following areas:

- **risk identification and assessment** – identifying the money laundering risks the Company is facing, given its customers, products, and services profile and having regard to available information, and assessing the potential scale and impact of the risks
- **risk mitigation** – identifying and applying adequate measures to mitigate the material risks the Company is facing
- **risk monitoring** – putting in place management information systems (MIS) and keeping up to date with changes to the risk profile through changes to the business or to the threats, and
- **documentation** – documenting the risk assessment and strategy, having policies and procedures covering the above and achieving effective accountability from the Board of Directors and Senior Management.

3.3. Customer Risk Assessment

Based on the information supplied at registration (e.g. customer's full name, residential address, geo-location, age, PEP/sanctions status), the Company will make an initial risk assessment of each customer. Customers thus start their gambling history with the Company categorise them as either Low, Medium or High risk for ML/FT. This will determine decisions made at later points in how they are dealt with. Customer risk assessments are made regularly and when new information obtained.

The customer risk assessment is based on:

- individual status (PEP, under sanctions, adverse media, etc.)
- geographical location
- gambling and transactional behaviour
- payment methods used by the player
- fraud red flags a customer triggered

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

3.3.1. Individual status

PEP

Politically Exposed Person means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level.

Any new or existing customer that is found to be a PEP or relative of such will have their account rejected or closed.

Sanctions lists

Governments and international authorities publish sanctions lists to combat persons engaged in illegal activities. Sanction lists include sanctioned people, organisations, or governments. Companies, individuals, organisations, or governments present on these lists as they may pose a higher risk.

Individuals and entities on these lists are subject to financial restrictions prohibiting counterterrorism regimes and money laundering worldwide.

Any new or existing customer that is found on the Sanctions database will have their account rejected or closed. Also, the MLRO must submit an STR to the Curaçao FIU.

Adverse media

Adverse Media or negative news is any bad and negative information about the customer or business discovered in various sources. This information can also expose someone being involved in a crime.

Any new or existing customer mentioned in adverse media can be a subject for EDD, but that depends on the finding. The Company may close the account or reject the registration depending on EDD results.

3.3.2. Geographical location

If the Company finds that the customer resides in a High-risk country, may be a subject for EDD.

High-risk countries are jurisdictions with serious strategic deficiencies to counter money laundering, terrorist financing, and proliferation financing. The Company defines the High-risk countries based on the FATF regulations (black and grey lists) and European Commission's list of high-risk third countries.

Link to the lists:

<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-counteracting-financing-terrorism-international-level_en

The Company has implemented a geoblocking tool to limit access to its services from players located in certain geographic locations.

3.3.3. Gambling and transactional behaviour

Each player's gambling and transactional behaviour is constantly monitored. The Company both looks for behaviours that are considered markers of harm for problem gambling and behaviours that can indicate money laundering/financing terrorism.

Behaviours, if noticed, were given allocated scores that combined with other scored ML/FT red flags.

If any examples of ML/FT behaviour are observed, then EDD check must be undertaken immediately of the customer and, if necessary, the SAR process implemented.

3.3.4. Payment Methods

Payment methods that allow the Company to trace the origin of the funds (such as a bank account) and to pay back to the source of the funds are considered low risk.

Payment methods that are funded by cash (or quasi cash), and does not allow the Company to trace the source of the funds are considered high risk.

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, Vouchers and Cryptocurrency	High

Manipulations with payment methods (e.g. deposits using one method, withdrawals using another) is also considered as a high-risk by the Company.

3.3.5. Fraud red flags

The Company has an anti-fraud risk management system to prevent bot attacks, fraudulent traffic, synthetic identities, account takeovers, identity thefts, credit card and CNP fraud, proxy users, multi-accounting, collusion etc. Some of the fraud red flags may also be connected to money laundering.

If the Company becomes aware a player triggered a fraud red flag, it will automatically be a subject for EDD.

3.4. Risk Score Calculation

Segment customers based on risk factors to detect potentially risky behaviour. Main factors include:

- **Geographical risk:** Customers from countries with high AML/CTF risks should be flagged. Know Your Country risk rating can be used. Please note that risk rating of countries is changing every 3 months. <https://www.knowyourcountry.com/ratings-table/>
- **Transaction behaviour:** Unusual deposit or withdrawal patterns (e.g., high-frequency, large sums). Deposit methods, Deposits VS Wager, Wagered last 12 months, Net hold last 12 months and Deposited amount last 12 months.
- **Gameplay patterns:** Identify players who exhibit irregular betting behaviour (e.g., high-risk betting, sudden spikes). Game type analysis (slots: low risk; roulette, BlackJack & live casino: high risk; sportsbook: medium risk).

Either of the categories implying a risk-based approach will provide an overall global risk score ultimately classifying whether the player is Low, Medium or High risk, which will then determine the actions need to be taken depending on that risk factor (*please see table below*). All scores are tallied up together and then divided by the number of triggers. For example if the player triggers deposit method as Skrill = 6, game type slots with score of 2, country Malta score of 4, deposit VS wager of 5x with a score of 6, deposit of 9,000 eur = 2, Net hold (NGR) of 3,000 eur = 1 and wagered 5 x 9000 score of 2 then the total score would be $23/7 = 3.28$ or 3 to the closest whole number therefore the global risk score would be a 3 (low risk).

AML Risk Profile	1	2	3	4	5	6	7	8	9	10
Global Score										

Please note: if multiple payment methods are used by the player that need to be calculated separately. For example: if the player used Skrill, Sofort and Visa, then the Deposit method overall score will be: $(6 + 6 + 4) / 3 = 5.33$ (5, so medium risk).

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

Not all factors can be automatically included in the CRA calculation due to technical or practical reasons, but the Company do monitor for these risks in other ways. For example, check for VPN usage or multi-accounting at the point of registration, there is a separate alert for players who use cards under a different name, and all withdrawals are checked before approval and payment.

3.5. 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
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

3.6. Additional Details & Source of Funds/Wealth

A daily report will be sent to the Company's Key Compliance Officer. The report will include any player who is newly classified as medium or high risk, or who has moved from medium to high risk.

The AML manager will then:

1. Review all accounts in the report, including:
 - a. Checking what information the Company already have on them
 - b. Carry out open-source checks
 - c. Checking if they are in any way suspicious
2. Take appropriate action (if necessary):
 - a. Block account if needed
 - b. Apply appropriate Due Diligence measures
 - c. Review the responses and the information provided by the player
3. If the player does not reply within 14 days, or the response is unsatisfactory, the account will be blocked. If documents are provided later, the AML manager should consider if the delay itself was suspicious, and act accordingly.

Accounts that have been assigned with medium or high risk, will require AML approval before any withdrawal request can be processed.

All decisions taken by the AML manager must be rectified and documented.

3.7. On-going Monitoring

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

- Obtain up to date identification documentation when existing documents have expired.
- Question the data and information about a player whenever inconsistencies are noticed.
- General review and update from time to time, based on customer's risk level.

3.8. Withdrawals

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

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

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 from the AML team before being approved and processed.

4. Customer Due Diligence

4.1. Purpose & scope

The Company distinguishes between Customer Due Diligence (hereinafter – CDD) and Enhanced Customer Due Diligence (hereinafter – EDD).

The customer is obliged to cooperate concerning the fulfilment of the due diligence request. If the Company cannot successfully carry out the due diligence, the business relationship won't be established or continued, and no transaction will be carried out. In addition, the Company examines whether it is necessary to submit a SAR.

4.2. Standard Customer Due Diligence

The Company applies general (standard) customer due diligence (hereinafter – CDD) measures to the customers at the registration stage. The CDD process consists of:

- identification – establishing identity by collecting information from the customer.
- verification – proving a customer is who they claim to be by obtaining and validating documents or information which supports this claim of identity, which come from a reliable and independent source.

According to the above requirements, The Company collects the following information for identification and verification to prevent money laundering and terrorist financing:

- a) First and Last Name
- b) Date of birth
- c) Residential address (street, no., ZIP code, city)
- d) ID
- e) Proof of Address (POA)

4.3. Documents acceptance

For acceptable ID documents, the Company require a government-issued document containing photographic evidence of the customer's identity. The following documents may be accepted for the verification purpose:

- current signed passport;
- driving license;
- identity card;
- another government issued document.

For POA verification the Company accepts:

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

The main requirements to the documents provided by the customer are:

- the document must be valid and not expired.
- documents must be clear, legible and of good quality.
- Mobile phone bills not be accepted, as they are not tied to a residential address.

4.4. Threshold approach

The Company may apply EDD measures in relation to any transaction that amounts to EUR 2,000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

“Transaction” consists of the wagering of a stake, including:

- the deposit of funds required to take part in remote gambling
- the collection of winnings, including the withdrawal of funds deposited to take part in remote gambling or
- winnings arising from the staking of such funds

The transactions are considered linked if they are part of the overall activity undertaken by a customer during a single period of being logged on to the operator's gambling facilities. However, this example is not exhaustive, and the Company considers other circumstances in which transactions are linked using a risk-based approach.

Consideration will need to be given as to whether there are other circumstances in which transactions are linked, such as, whether a customer is deliberately spreading their wagering or collection of winnings over a number of transactions in order to circumvent the CDD/EDD requirements.

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

4.5. Ongoing monitoring

The general due diligence duties include the ongoing monitoring of the business relationship. This includes:

- Obtaining up to date identification documents when existing documents have expired.
- Questioning the data and information the Company hold about the player, whenever inconsistencies are noticed.
- General review and update from time to time, on a risk sensitive basis.
- Checking if transactions are matching with the information and documentation available at the Company about the customer.
- Updating the respective documents, data, or information at appropriate intervals, based on the customer's risk level.

4.6. Enhanced Due Diligence

The Company applies Enhanced Due Diligence measures (hereinafter – EDD) and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the money laundering or terrorist financing risks.

EDD is applied in the following cases:

- in any case, identified by the Company or in the information provided by the authorities to the Company where there is a high risk of money laundering or terrorist financing;

- if the Company has doubts as to whether the information collected regarding the identity of the customer is not correct or not (or no longer) accurate;
- if the Company has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP;
- in any case where the Company discovers that a customer has provided false or stolen identification documentation or information, and the Company proposes to continue to deal with the customer;
- in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, or the transaction or transactions have no apparent economic or legal purpose,
- in any other case which, by its nature, can present a higher risk of money laundering or terrorist financing.

In cases where there is a higher risk, establishment of the business relationship or continuation of the business relationship (if the higher risk only arose later or was only recognised later) can happen only with the consent of the Key Compliance Officer.

If a customer has been deemed to be a high-risk or becomes one at any stage, the Company undertakes the EDD procedure, including any of the below (depending on the case):

- Re-verification of identity (repeated CDD).
- Establishing how the customer acquired his wealth to be satisfied that it is legitimate:
 - salary income or company profit (Certified Payslip / Certified employer letter / audited accounts if self-employed);
 - sale or liquidation of financial instruments (Certified shares/investments sale contracts or statements/ accountant letter);
 - sale of property (Certified copy of the contract of sale or letter from a solicitor or estate agent);
 - inheritance (Certified copy of will including the value of heritage);
 - sale of the company (Certified contracts, media articles, certified letter from accountant or solicitor), etc.
- Establishing the customer's source funds to be satisfied that they do not contain the proceeds of crime.

- Ensure that deposits originate from payment methods that belongs to the customer and do not allow anonymity by requesting copies of bank statements or account statements.
- Undertaking increased continuous monitoring of the business relationship.
- Any suspicious transaction must be investigated, and the business relationship underlying the transaction shall be monitored to assess the risk of money laundering and terrorist financing.

With EDD checks on transactions, the Company's fundamental aim is to ensure the transparency of payment flows. Accordingly, the origin and destination of the money used in a transaction shall be traceable back in each case to an account.

Definition of Source of Funds

The Source of Funds refers to the origin of the particular funds being used to deposit on the Company's website. This is not simply verifying which bank or financial institution the customer may have received the funds from. The information obtained should be substantive, relevant and establish the fund's origin and the method/circumstances under which the funds were acquired.

Definition of Source of Wealth

The Source of Wealth refers to the origin of the entire body of wealth (i.e. total assets) of the client. The information that the Company obtains should indicate the volume of wealth the client would reasonably be expected to have and provide a picture of how it was acquired.

4.7. Politically Exposed Persons and Sanctions Screening

The Company uses a 3rd party KYC software to check all new customers at the registration stage against PEP and Sanctions databases. Customers screened against the following sanction lists:

- OFAC (Office of Foreign Assets Control);
- EU (European Union);
- OFSI (Office of Financial Sanctions Implementation);
- UN (United Nations); and
- Australian Governments Dept. of Foreign Affairs (DFAT).

Any new or existing customer found on the Sanctions database, or a PEP (or relative of such) will have their account rejected or closed.

In case of identifying a PEP, responsible staff will send a report to the Key Compliance Officer who in turn will send a report to the Senior Management.

The Key Compliance Officer will investigate each case to identify positive or false-positive PEP alert. The Company has a right to request additional documents from the customer for this purpose within the investigation.

If the PEP alert is true-positive, the Key Compliance Officer will reject the registration or close the account and inform the Senior Management about the decision taken.

Politically Exposed Person means any person who has been entrusted with a high-ranking prominent public function at the international, European, or national level or who is or has been entrusted with a public position of comparable political importance below the national level. In particular, politically exposed persons are:

- heads of state, heads of government, ministers, members of the European Commission, deputy ministers and assistant ministers,
- members of parliament and members of similar legislative organs,
- members of the governing bodies of political parties,
- members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are usually not subject to further appeal,
- members of the boards of courts of audit,
- members of the boards of central banks,
- ambassadors, chargés d'affaires and defence attachés,
- members of the administrative, management or supervisory bodies of state-owned enterprises,
- directors, deputy directors, members of the board or other managers with a comparable function in an international or European intergovernmental organisation.

Family member of PEP means a close relative, in particular

- the spouse or civil partner,
- a child and the child's spouse or civil partner and
- both parents.

4.8. Procedure for Account Closure

The Company may decide to close a customer's account on any of the below reasons:

- Fraud;
- Cheating;
- Bonus Abuse;
- Allowing a third person to use their account;
- Under-aged gambling;
- Problem gambler;
- Being abusive to staff;
- Commercial concerns;
- CDD/EDD failure;
- Terms and Conditions breach.

By law the Company must end the business relationship with the customer unless obtained appropriate consent for it to continue and even then, it is precautionary to close the account.

Due to the laws on Tipping Off, the Company cannot inform the customer that it has concerns regarding ML/FT, thus account closure must be done sensitively.

The Key Compliance Officer will need to consider whether if a SAR should be submitted as part of the concern about the player's behaviour whether appropriate consent should have been requested.

Where the Company is unable to complete or apply the required CDD measures in relation to a particular customer at the point the CDD threshold for transactions is reached, and is accordingly required to cease transactions and terminate the business relationship with the customer.

4.9. Corporate Customers (B2B)

For Corporate customers, the company will automatically require Enhanced Due Diligence for all UBOs and Directors holding 10% or more shares in the shareholding capacity of the customer's company. In order to assess whom, the Directors and UBOs are, the company will require the following documents;

- Memorandum of Association
- The company's Excerpt of the Registrar / Chamber of Commerce
- Registry of Directors
- Registry of Shareholders
- Active Gaming License or Declaration with Business plan on the attempt to obtain a Gaming License
- AML Policy

In addition to this, the AML Officer may, at their discretion, request any of the required documents to be Notarized and/or Apostilled. Corporate customers are automatically considered as high risk and are subject to quarterly due diligence review by the AML officer.

5. Funds Management Procedures

5.1. Player Account Balance

All funds deposited by the player or owed by the Company are credited to the player's corresponding account. The player can top up the funds in his/her account by depositing through the cashier on the Company's website and then use these funds to place bets. Bets are deducted from the account balance, and winnings are added to the account balance.

The player can withdraw withdrawals of available funds in the player's balance. The Company do not offer credit to players. A player may not transfer funds to another player.

5.2. Payment Methods

Payments shall only be accepted and made from accounts held with licenced financial institutions or through licenced payment providers.

No cash deposits/withdrawals will be affected between the Company and its players.

5.3. Player Deposits

After registering a gaming account, a player may then deposit funds into their account through the cashier on the site.

In order to facilitate these deposits, the company has integrated a number of gateways. All gateways are PCI DSS compliant, and the company does not hold any credit card data itself.

The company submits the transaction to the PSP and then waits for approval from the card acquirer/e-wallet. On approval, the deposit status is updated and the funds added to the player's balance.

5.4. Player Withdrawals

A player with an available balance will be able to request a withdrawal of the funds via the cashier on the site. The player will enter the amount they wish to withdraw and select their preferred payout method. The withdrawal amount is then deducted from the player's balance.

5.5. Withdrawal Payouts

In remitting funds to the player, the Company will, where possible, remit the funds directly into the account where the funds originated from, keeping a closed loop.

Provided that where this is not possible, the Company will remit the funds to the player in line with the requirements under AML legislation and to the lowest risk method possible.

6. Crypto payments

6.1. Compliance with regulatory requirements

Bonus Operations N.V. is committed to ensuring compliance with all applicable regulations governing Virtual Financial Assets (VFA). This includes adherence to Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) regulations, as well as other relevant financial regulations.

The Company will implement and maintain robust systems and controls to prevent the use of Virtual Assets for illicit activities. This includes conducting thorough due diligence, monitoring transactions, and reporting any unusual activities to the Curaçao Gaming Control Board (GCB) and Curaçao FIU. This part outlines the use and acceptance of VFAs, complying with applicable laws and regulatory standards, in particular, VFAs that involve the use of Distributed Ledger Technologies (DLT).

6.2. Risks with crypto payments

Cryptocurrency is decentralized digital money secured by cryptography and based on blockchain technology - that is, a distributed digital ledger that keeps a secure, transparent, and decentralized record of transactions.

Cryptocurrency is almost impossible to counterfeit or double-spend, so it might prove valuable to online gambling sites looking to become more secure and transparent.

However, their decentralized structure allows crypto to exist outside the control of governments and central authorities. Therefore, this new form of value is extremely unregulated.

Risks using cryptocurrency:

- Lack of legal framework;
- Volatility;
- Hacking concerns;

Cryptocurrency is an exciting, technology-powered form of value that promises to change many aspects of people's lives - including their gambling habits. However, while promising, this technology is still riddled with loopholes and issues that need to be addressed to protect consumers and the gambling industry as a whole.

Apart from focusing on all the benefits of digital currencies, Bonus Operations N.V. is aware of its potential risks and do its best to mitigate them.

6.3. Unhosted wallets

Unhosted wallets, defined as digital wallets that are not managed or hosted by a third-party service provider, are subject to stringent transparency requirements. The Company is aware that transparency regarding the owner and beneficiary of unhosted wallets is paramount for regulatory compliance and mitigating risks associated with Money Laundering (ML) and Terrorist Financing (TF).

Bonus Operations N.V. will ensure that players utilizing unhosted wallets for gaming transactions provide comprehensive information regarding their identity, including but not limited to, full name, address, and official identification documents. The Company will conduct thorough due diligence procedures to verify the identity of unhosted wallet owners, in line with established AML & CFT standards. Any unusual activity or transactions that raise concerns regarding the source or destination of funds will be promptly reported.

6.4. Custodial wallet services

Custodial wallet services, facilitating the exchange of Virtual Currencies (VC) to fiat, vice versa, or VC-to-VC transactions, are subject to rigorous monitoring and compliance measures to mitigate risks associated with money laundering and terrorist financing.

The Company when offering custodial wallet services through third-party Custodial Wallet Providers, will implement robust Customer Due Diligence (CDD) procedures to ascertain the source of funds (SOF) and verify the identity of users engaging in VC transactions, including minimum age requirements. Comprehensive KYC (Know Your Customer) protocols will be established to collect relevant information, including personal identification details and transaction histories, from customers. The Company will implement effective transaction monitoring systems to detect and prevent suspicious activities within custodial wallet services.

6.5. Volatility of VFAs

The values of VFAs relative to fiat currencies (e.g. EUR) may be subject to significant volatility and fluctuation. As a result, the value of VFAs may increase or decrease substantially over a short period of time. The Company hereby advises all players that VFAs are subject to significant fluctuations in value (vis-à-vis fiat currencies) due to market volatility. By engaging in transactions involving VFAs, all players acknowledge and accept the inherent risks associated with such volatility. Players are strongly encouraged to exercise caution and to consider these risks when making deposits, withdrawals, or any other financial transactions involving VFAs. All players acknowledge that due to the risks associated with the volatility of the value of VFAs relative to fiat currencies, that they may deposit or withdraw a sum which is higher or lower in value when compared to fiat currencies than anticipated.

7. Suspicious Activity Reporting

7.1. Purpose & scope

Every employee of the Company must report to the Key Compliance Officer if there is a suspicion or knowledge of money laundering, funding of terrorism or if the funds being used on the Company's website are the proceeds of criminal activity.

The Key Compliance Officer will consider each report and determine whether it gives grounds for knowledge or suspicion. If they do, then a SAR should be submitted to the Financial Intelligence Unit (hereinafter – FIU or FIU Curaçao).

Knowledge means that the person reporting knows the event to be a fact. Suspicion implies that the person reporting the incident may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial or financial sense.

A transaction or activity may not be suspicious at the time, but if suspicions are raised later, an obligation to report the activity then arises. Likewise, if concern escalates following further enquiries, it is reasonable to conclude that the transaction is suspicious and will need to be reported to the FIU.

The Key Compliance Officer will assess all the circumstances related to the suspicion. Decision making will depend on what is already known about the customer and the transaction and how easy it is to make further enquiries.

7.2. Red Flags / Indicators

Red flags are not intended to automatically result in filing a SAR with the FIU, however, are merely indicators that should lead the Company to question the customer's behaviour. If there is no reasonable explanation for the red flags, then an internal report must be made to the Key Compliance Officer.

The following is a list of possible red flags which should be considered:

- Customer does not cooperate in the carrying out of CDD/EDD.
- Customer attempts to register more than one account on a site.
- Customer makes small wagers, even though the amounts deposited are significant, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.

- Noticeable changes in the gaming patterns of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions, he/she normally carries out.
- Customer enquiries about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate when seen in the context of what is known about the Customer's wealth, income or financial situation.
- Customer seeks to transfer funds to a bank account held in the name of a third party.
- Customer requests a withdrawal to an account he/she never deposited with.
- Customer opening an account and registering several different cards and making transfers between them.
- Customer depositing large sums, then places minimal bets, then withdrawing all their funds.
- Customer depositing large amounts and repeatedly losing large amounts as if the loss is of no consequence.

7.3. Inability to Complete CDD Measures

If a customer refuses to provide CDD/EDD documentation, the Company won't immediately equate this on its own to suspicion of ML/FT.

The Company will consider all factors and information, including the payment method(s) used, game(s) played, playing trends and patterns, jurisdiction, and any open-source information.

If there are grounds to suspect ML/FT after considering all of these factors, then an SAR must be submitted.

7.4. Internal Suspicious Activity Report

All employees have a duty to report suspicious transactions / activity. If an employee has any suspicion about a customer's behaviour or transaction, it must be reported to the Key Compliance Officer immediately. For this purpose, employees use the Internal Suspicious Activity Report Form.

The employee should still submit the report, even if their superiors are not in agreement. It will then be up to the Key Compliance Officer to determine if the information available can be considered sufficient for a SAR to be filed to the FIU.

The following information is included in an Internal SAR:

- The customers details;
- The member of staff's statement about what gave them cause to make the report;
- All relevant documentation and information.

The Key Compliance Officer will:

- Acknowledge receipt of the report, review and investigate further as required;
- Make an assessment based upon all the information and decide whether the matter needs to be reported externally to the FIU
- Make a record about the decision taken.

7.5. External report to FIU

Once the Key Compliance Officer has received an Internal SAR, she/he will decide if a SAR should be submitted to the FIU.

When making this decision, the Key Compliance Officer should consider that AML legislation is intended to address serious crime which usually either involves amounts that are not minimal or circumstances that show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes.

For example, identity fraud and chargebacks may give rise to ML, but a licensee will only be subject to reporting obligations if they result in funds derived from these activities being deposited with or held by the licensee.

However, the Company won't report single instances involving small amounts but should consider whether it can detect a more significant pattern or scheme.

The Key Compliance Officer considers whether an internal report gives rise to a suspicion of ML by taking into account all relevant information, including assessing whether there are common denominators between e.g., repeated suspicious behaviour, instances of chargebacks or identity fraud. For example, these may consist of common or related persons, common IP addresses etc.

The Key Compliance Officer, in deciding to submit the SAR or not, should answer the following questions:

- Who is involved?
- How are they involved?
- What is the criminal/terrorist property?
- What is the value of the criminal/terrorist property (estimated as necessary)?
- Where is the criminal/terrorist property?
- When did the circumstances arise?
- When are the circumstances planned to happen?
- How did the circumstances arise?
- Why you are suspicious or have knowledge.

7.6. Reporting Procedure

The Company is obliged to submit a suspicious activity report to the FIU, through the user interfaces on the FIU's website or by mail (if possible), without due delay if there are indications that:

- the Company know, suspect, or has reasonable grounds for knowing or suspecting money laundering and/or terrorist financing,
- an asset related to a business relationship or transaction originates from a criminal offence that could constitute a predicate offence to money laundering,
- a business case, transaction, or asset is related to terrorist financing.

When the Company decides whether it is necessary to submit a SAR, it takes the following factors into account, including but not limited to:

- the purpose and nature of the transaction,
- peculiarities of the customer,
- the financial and business background of the customer,
- the origin of the assets contributed or to be contributed.

The Company doesn't execute suspicious transactions, except in cases where it cannot postpone the transaction or if the postponement could hinder the prosecution of an alleged criminal offense. In this case, the Company submits a SAR immediately.

7.7. Tipping-off

It is an offence to inform anyone that a SAR 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 employees of the Company shouldn't:

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

8. Internal Controls

8.1. Purpose & scope

The Company has a number of internal controls and general procedures which will be used on a day-to-day basis in respect of managing and running the daily operations of the business. The main purpose is the prevention of money laundering and terrorist financing.

8.2. Recordkeeping

The Company keeps all the documents and data collected or obtained within the scope of the due diligence, including:

- all data and information used to identify and verify customers (including type and number of the document, issuing authority, etc.);
- all records (receipts) relating to transactions, i.e., 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, as well as the documentation on the appropriateness of the measures taken based on these results;
- the results of internal investigations, communication with FIU and regulators;
- documents collected within the scope of business partners due diligence;
- documents collected from the employees within the scope of the due diligence;
- documents regarding AML trainings (training materials, examination results, etc.);

The Company also keeps all documents created and processed in connection with a suspicion of money laundering or terrorist financing, including:

- all related internal and external correspondence, files and interview notes;
- the results of internal investigations and the measures taken, that can explain why the MLRO concluded and initiated the actions taken.

The retention period is ten years and starts with the end of the calendar year in which the business relationship ends and in all other cases with the end of the calendar year in which the respective information was ascertained. Applicable legislation may provide for a more extended retention period. The Company destroys all the documents and data collected after retention period expiration unless other recordkeeping or retention obligations apply, but not less than 10 years.

8.3. Money Laundering Reporting Officer

The Company has appointed a Key Compliance Officer whose main responsibility is to review any internal suspicious transaction reports, and where necessary to submit a SAR with the FIU. The Key Compliance Officer is the main contact point for the FIU.

In order to ensure that the Key Compliance Officer is able to fulfil their role effectively, the Company guarantee that:

- Key Compliance Officer acts independently, has been provided the necessary knowledge of the Company's activities and is able to decide independently as to whether internal reports are to be escalated to the FIU.
- Key Compliance Officer has no conflicting responsibility which may pose a conflict of interest.
- Key Compliance Officer has sufficient time, resources and information to fulfil their responsibilities.
- Key Compliance Officer has a right to create work assignments to relevant employees and take decisions regarding ML/TF prevention.

The Key Compliance Officer and their deputy carry out the following functions (including but not limited to):

- Creating and further developing the internal risk analysis, including a complete scope of risks connected to money laundering and terrorist financing.
- Developing and updating internal policies and procedures to prevent money laundering and terrorist financing.
- Creating unified reporting channels.
- Involvement in other internal organizational and work instructions creation and their further development, related to implementing the regulations on the prevention of money laundering or terrorist financing.
- Ensuring compliance with current AML regulations, and other relevant legislations.
- Ongoing monitoring of the Company's business activity to comply with the anti-money laundering regulations.
- Ensuring CDD/EDD is undertaken.
- Suspicious activity risk assessment.

- The submission of SARs in appropriate cases.
- Contributing to the content of staff's AML training.
- Maintaining a list of all inquiries received from law enforcement agencies and records relating to internal and external disclosures.
- Submitting a report to the management on Key Compliance Officer activities on the risk situation of the Company and the measures taken and intended to implement the obligations under money laundering regulations.

The Key Compliance Officer and their deputy are authorized, within the scope of their performance of their work:

- To perform their tasks independently and effectively.
- To submit the necessary legally binding declarations for the undertaking and represent it externally in relevant situations.
- To provide undertaking-specific instructions for all matters relating to the prevention of money laundering and terrorist financing.
- To carry out random checks without restriction.

8.4. Training

The Company will provide training to all staff directly or indirectly through a service provider upon joining the Company and after that annually.

Relevant training materials will be prepared for all teams based on Company policies, which is compiled according to the applicable legislation requirements and guidelines.

Training will be conducted as follows:

- Training material based on the finalised and approved Company policies, in the form of documents and presentations.
- Training will be provided to existing management and staff.
- Training will also be included in the induction of all new staff.
- Training will be followed up with a questionnaire to test everyone's understanding.
- Should the Company find that some parts of the training are unclear it will repeat the training focusing on the issues that were not understood.

- Regular refresher training will be given, which will include any updates and will focus on any shortfalls that arose during the previous period.
- Any update in the AML policy will be communicated in a group email and through ad-hoc training, and added to periodic training updates and material.

Staff training will focus on ensuring awareness of:

- all applicable legislations,
- the provisions of the money laundering and terrorist financing requirements,
- staff personal obligations under the money laundering and terrorist financing requirements,
- applicable internal reporting procedures,
- Company's policies and procedures to prevent money laundering and the financing of terrorism,
- Company's identification and verification procedures, record-keeping, and other procedures to prevent money laundering and the financing of terrorism,
- recognition and handling of suspicious transactions,
- staff personal liability for failure to report information or suspicions under the money laundering and terrorist financing requirements and the Company's internal procedures,
- new developments, including information on current techniques, methods, and trends in money laundering and the financing of terrorism,
- the money laundering and terrorist financing risks faced by the Company, and
- Data protection regulations.

Induction training sessions will be conducted for all employees and will include fraud prevention, detection and ancillary methods, as required by their role. Refresher training will also be provided, both on a regular basis and as needed, so as to keep employees up to date and informed of the Company's policies and procedures and any changes or improvements made. The MLRO keeps records of training delivered, showing details of the training has been provided, when and by whom, and the next training date. In case of any changes to the Company's policies and procedures or applicable legislation, all staff will get the relevant training.

8.5. Employees background check

Prior to engaging employees, the Company will carry out relevant integrity checks, in-line with their position, responsibilities and access levels. The Company will not employ any persons who are not deemed to be fit and proper.

For this purpose, the Company may request the following documents (in each case with due regard to data protection):

- a valid, original identity document,
- up to date CV,
- any other documents, as the Company deems necessary to request.

Once a person is employed, screening shall still be carried out on an ongoing basis as required. All employees of the Company must guarantee that they observe the provisions of applicable legislation and the associated due diligence obligations, report facts relevant to money laundering, and do not themselves participate actively or passively in dubious transactions.

For this purpose, Senior Management will regularly carry out checks on employees or whenever the Company feels the need to perform such inspections. In particular, such inspections shall be carried out when suspicion arises concerning the behaviour of specific employees. The Company may carry out these checks through surprise spot checks or other procedures that will enable such personnel to verify whether employees comply with the policies and procedures.

The frequency and extent of screening that shall be carried out, must be proportionate to the risk level posed by the employee. The risk level will be determined case by case depending on employee's position (e.g., head of department, senior, mid), the scope of duties and obligations, etc.

The Company will check all the employees at least once a year. The Company will use an employee performance sheet for this purpose.

8.6. Internal and external revision and staying up to date

The Company has compiled its policies and procedures according to the requirements of the applicable legislation and guidance of the FATF, GCB and FIU. However, the requirements and guidance, as well as external fraud trends, can and will change. Therefore, the Company has implemented the following measures to ensure the relevance of the Company's internal AML documentation:

- Key personnel have subscribed to mailing lists offered by the FIU, GCB and FATF and joined relevant forums
- The Company periodically takes legal advice from the gambling consultants for AML best practices
- In the case of an update, the Company will take the following steps, as necessary:
 - Update Company's policy documentation and training material
 - Inform all relevant staff by email regarding the updates, meet with relevant team managers, and ensure they update their departments appropriately
 - Update email communication templates and chat canned responses
 - Update website policies, maintaining a version number and 'last update' date
 - Update the Terms and Conditions, maintaining a version number and 'last update' date.

Any consequential update to the Terms and Conditions will trigger a pop-up notification to players on their next login, where they need to accept and agree to the new version before proceeding.

The Company may engage a third-party service provider with expertise in AML compliance to conduct independent external reviews of the Company's AML policies and procedures. The results of these reviews will be reported to the Senior Management and used to enhance AML/CTF measures and documents as needed. The frequency of external reviews are determined by the Senior Management. It may be conducted annually or more frequently, depending on the need for an updated assessment of the Company's AML program's effectiveness.

8.7. Version Control

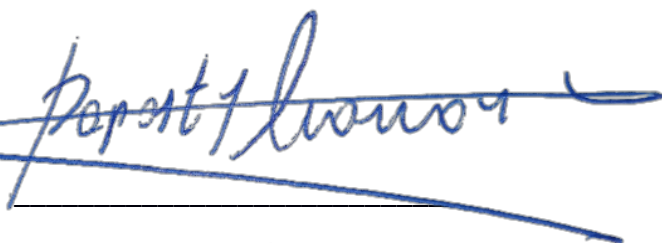
The Company is constantly improving its AML/CFT Policy in order to actively combat Money Laundering and the Financing of Terrorism. Therefore, it requires version control to keep track of said changes and approval by the Board of Director(s).

Version	Date	Author	Approved By
1.0	29.05.2025	Bonus Operations N.V.	Director(s) and the Key Compliance Officer

Bonus Operations N.V
Curacao, 29 May 2025



Capital Trust Corporation N.V.
Managing Director



Georgios Papastylianou
Key Compliance Officer