

NovaPlay N.V. (Curaçao) AML/CTF/PF

POLICY AND PROCEDURES v1.0

Version Number	V1.0
Status	Active
Authorization and approved by	
Review	Annual
Next review date	

Effective date	Version	Comments
13/10/2025	v.1.0	Document creation

Table of Contents

1. POLICY APPROVAL	5
2. GENERAL PROVISIONS	6
3. LAWS & REGULATIONS	7
4. DEFINITIONS	8
MONEY LAUNDERING	8
PROLIFERATION FINANCING	8
TERRORIST FINANCING	9
HIGH RISK COUNTRY	9
POLITICALLY EXPOSED PERSON (PEP)	10
SANCTIONS	10
FIAT CURRENCY	10
CRYPTO (DIGITAL) CURRENCY	10
5. RISK BASED APPROACH	11
BUSINESS RISKS (BRA)	11
CUSTOMER RISKS (CRA), PRODUCT RISKS (PRA), TECHNOLOGY RISKS (TRA)	11
6. CUSTOMER DUE DILIGENCE	12
DUE DILIGENCE	12
BENEFICIAL OWNERSHIP	14
PEPs & SANCTIONS:	14
ENHANCED DUE DILIGENCE	16
SIMPLIFIED DUE DILIGENCE	18
THE TERMINATION OF THE BUSINESS RELATIONSHIP	19
ONGOING MONITORING:	20
7. CRYPTOCURRENCY TRANSACTIONS	21
DEPOSITS & WITHDRAWALS:	21
CRYPTOCURRENCY TUMBLERS & MIXERS	23
8. REPORTING SUSPICIONS AND UNUSUAL TRANSACTIONS	25
SUBMITTING A FORMAL UNUSUAL (SUSPICIOUS) TRANSACTION REPORT	26
9. RECORD-KEEPING	28
10. ANTI-MONEY LAUNDERING PROGRAM	28
INTRODUCTION	28
INTERNAL POLICIES, PROCEDURES AND CONTROLS	29

THE APPOINTMENT OF A COMPLIANCE OFFICER	29
THE EMPLOYEE SCREENING AND ONGOING TRAINING PROGRAM	30
AN INDEPENDENT AUDIT FUNCTION	30
11. RESTRICTED JURISDICTIONS	31

1. POLICY APPROVAL

NovaPlay N.V. (the 'Company') is a company registered and incorporated in Curaçao with Company registration: 171648.

The Company is committed to ensuring that it takes all appropriate steps to prevent its systems from being used for the purposes of money laundering, terrorist financing or other crime. These steps include, but are not limited to;

- the appointment of a suitably qualified Anti-Money Laundering & Compliance Officer
- board approved policies and practices
- risk-based approach to all business relationships
- applying appropriate use of technology and tools to help identify and mitigate risk
- ensuring all employees are suitably trained
- reporting suspicious activity to relevant law enforcement agencies
- an annual independent audit of its Anti-Money Laundering Compliance Program

This document has been produced to ensure that the Company acknowledges and applies appropriate measures to address the higher level of risks associated with the business.

This document has been reviewed and approved by a resolution of the Management Board of the Company.

All future versions and updates will be reviewed by the Management Board before being approved and issued.

The latest version of this document will replace all previous versions within the Company's operations.

All changes, additions and approvals to this policy will be captured in the tracking tables on page 2 for the record purposes.

2. GENERAL PROVISIONS

The Company is licensed and regulated by the Government of Curaçao to offer interactive (online) remote betting and gambling products (games of chance) and services under Supplier license issued by The Curacao Gaming Control Board (GCB) with:

Gaming License Number: QPA/2025/04178

In accordance with the National Ordinance on Games of Chance (Landsverordening op Kansspelen, "LOK

Under the terms of its operating license the Company is required to have in place adequate policies, processes and procedures to prevent its systems from being used for the purposes of money laundering, proliferation financing, terrorist financing or other criminal activity.

This document will be reviewed on both a regular basis and ad-hoc basis as required by changes to laws and regulations, changes to license conditions, introduction or implementation of new products and services or in accordance with the Company's risk management practices and procedures.

3. LAWS & REGULATIONS

The designated supervisory Authority for service providers offering their services from the jurisdiction of Curaçao, or under a license issued by the (Curaçao Gaming Authority)

The Company is required to comply with all applicable laws and regulations, including:

- The National Ordinance Criminal Code (P.B. 2011, no. 49);
- The National Ordinance of November 23, 2015 amending the National Ordinance identification for services (P.B. 2015, no. 69);
- The National Ordinance on Identification when Rendering Services or NOIRS (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92); and
- The National Ordinance on the Reporting of Unusual Transactions or NORUT (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).
- Sanctions National Ordinance
- Kingdom Sanction Act
- Ministerial Decree on Indicators of Unusual Transactions
- National Decree – Kingdom Sanction Law Enactment

These Ordinances require that all service providers offering online games of chance (including but not limited to sports-betting and casinos) from the jurisdiction of Curacao must have in place adequate practices and procedures to prevent the Company and its systems from any activity that facilitates money laundering, proliferation financing, funding of terrorism or other criminal activities.

4. DEFINITIONS

MONEY LAUNDERING

Money laundering is defined as:

- the conversion or transfer of funds or property derived from criminal activity;
- retaining funds or property derived from criminal activity;
- participation in such activity such as for the purposes of concealing, or disguising the illicit origin of the funds or property or assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions;
- acquisition, possession or use of funds or property derived from criminal activity, or property obtained instead of such funds or property, knowing, at the time of receipt, that such funds or property was derived from criminal activity or from an act of participation;
- the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, funds or property derived from criminal activity.

Furthermore, Money Laundering consists of three phases:

- **Placement.** During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- **Layering.** This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- **Integration.** The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

PROLIFERATION FINANCING

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical, or biological weapons and their means of delivery and related materials.

TERRORIST FINANCING

Terrorist financing is defined as:

- the allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organizations, or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

PROLIFERATION FINANCING

In October 2020, the Financial Action Task Force revised its standards (R1 and INR 1) to require Countries, Financial Institutions and designated non-financial businesses and professions to identify, assess, understand and mitigate their Proliferation Financing risks.

Proliferation financing ("PF") refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligation.

According to FATF, PF risk indicators include those relating to;

- Customer Profile
- Account and Transaction history
- Maritime sector risk indicators
- Trade Finance

Further guidance on PF risk indicators, issued by FATF, can be found at [Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf \(fatf-gafi.org\)](https://www.fatf-gafi.org/publications/fatfguidance/documents/guidance-proliferation-financing-risk-assessment-mitigation.pdf)

Staff should familiarise themselves with the typologies and red flag indicators of PF as documented by FATF, in order to identify circumstances in which customers and transactions may present PF risks. Any risks identified will be mitigated by such measures as;

- a. Sanctions screening to identify any potential sanctions evasion.
- b. Enhanced customer due diligence procedures;
- c. Effective maintenance of customer master data;

d. ongoing compliance monitoring

HIGH RISK COUNTRY

A high-risk country is defined as:

A country or territory where the risk of money laundering, terrorism or financial or other crime is considered to be higher than other countries or territories, as may be determined by organizations such as:

- European Union
- United Nations
- Financial Action Task Force (FATF)
- Moneyval
- International Monetary Fund (IMF)
- US Office of Foreign Asset Control (OFAC)

The term high risk can be applied to either the country or jurisdiction or to nationals, citizens or residents of the country or jurisdiction. Equally, nationals, citizens or residents of high-risk countries or jurisdictions may be subject to Sanctions checks preventing or limiting a business relationship.

POLITICALLY EXPOSED PERSON (PEP)

A Politically Exposed Person is defined by the National Ordinance on Identification when Rendering Services (NOIRS) as:

- an individual or person who holds or has a prominent public function with the exception of those who have held this position for less than a year, and the immediate family members or close associates of these persons.

SANCTIONS

Sanctions may be imposed on countries, companies or individuals.

Sanctions listed individuals are defined as:

- individuals subject to regulatory or financial sanctions or enforcements, known terrorists, money launderers, fraudsters and black-listed persons.

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly, or indirectly, to or for the benefit of any designated persons or entities.

FIAT CURRENCY

Fiat currency is currency that is issued and declared to be legal tender by a national government such as British pound, or a political or economic coalition such as the EU and the Euro.

It is issued by a central authority and whilst transactions can be peer to peer most electronic transactions are facilitated by a third-party payment processor.

5. RISK BASED APPROACH

The Company is committed to taking a risk-based approach through its Anti-Money Laundering Compliance Program. Its primary goal is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The company will implement a set of policies and practices to identify and mitigate risks including:

- identify and assess the level of risk (low to high)
- assess the impact of risks identified
- identify and implement controls to mitigate against the risk and its impact
- ensure on-going monitoring to evaluate and ensure the effectiveness of the controls
- periodically review and update its risk management policies and processes in accordance with events, the introduction of new products or technology or changes in laws and regulations.

The company will conduct a full assessment in relation to identifying and implementing controls to mitigate:

BUSINESS RISKS (BRA)

The compliance officer will perform a review of all of the ML/FT/PF risks that the business faces and document such risks in the Business Risk Assessment. The Business Risk Assessment will record the identified risks, the assessment of these risks and the controls and mitigations in place to prevent such risks from materialising.

In identifying and assessing risk, consideration will be given to factors such as;

- Regulatory environment and potential changes
- National Risk Assessments relating to Curaçao
- The type of business undertaken by the client
- Product/service offered to the client

The risk assessment will include the following:

- A description of the risk
- The probability of the risk occurring and the impact it will have on the Company
- A description of the mitigations and controls in place to reduce the risk

The Business risk Assessment will be reviewed at least annually and when circumstances change or new threats emerge.

In order to identify emerging risks for inclusion in the Business Risk Assessment, the Compliance Officer will compile an annual compliance report which will include findings from review of relevant law enforcement alerts and reports, thematic reviews issued by the relevant regulatory bodies in Curaçao and industry specific risk guidance.

CUSTOMER RISKS (CRA)

The Company is required to have and follow reasonable procedures to document and verify the identity of customers prior to establishing a business relationship with them.

All customers are to undergo a full risk assessment prior to being onboarded as a client.

Customers are categorized as either low, standard or high risk. Below is the criteria for each risk rating.

High Risk:

- The business relationship is conducted in unusual circumstances
- The customer is a resident or transacts with a geographical area of high risk
- The corporate structure of the customer is unusual or excessively complex given the nature of the company's business
- Politically exposed person (PEP)

Where a customer is deemed to be high risk, they will undergo enhanced due diligence (EDD) checks with additional ongoing monitoring.

Low Risk:

Any company whose securities are listed on a regulated market will be considered as low risk. A Low -Risk client will undergo standard CDD checks and ongoing monitoring.

Standard Risk Customer

Any customer who does not have any high- or low-risk factors will be classified as standard risk. This category will undergo standard CDD checks and ongoing monitoring to assess any changes which may lead to the client being recategorised as high risk.

Technology Risk Assessment (TRA), Product Risk Assessment (PRA)

The Company will undertake a risk assessment of any new technology it intends to use in the business or any products it intends to distribute. The potential risks will be considered under the following categories.

- Operational risks: Losses that may arise due to deficiencies in system reliability or integrity. This will also take into account how the product interacts with customers and the methods in which payments for the product are received.
- Reputational risks: Negative public reactions caused by system or product failure
- Legal risks: Failures resulting in violations or non-compliance with legislation.

An assessment will be performed for each new technology and will cover risk identification, vulnerability, consequence and mitigation.

A log of all risk assessments undertaken will be maintained by the Compliance officer and will be presented to the board annually. All risk assessments will be documented appropriately detailing the measures undertaken and the reason for the assessment.

6. CUSTOMER DUE DILIGENCE

The Company will apply appropriate customer due diligence measures to all customers in accordance with applicable laws and regulations. As NovaPlay operates on a **B2B basis**, providing games and related services to licensed Operators & Aggregators rather than directly to players, due diligence will focus on the identification and verification of these B2B customers. Where relevant, initial due diligence will also include checks relating to technical identifiers due to the digital and virtual nature of the services provided.

The Company shall use a risk based approach when undertaking ongoing customer due diligence, in accordance with this policy and the customer risk assessment.

The Company shall perform CDD prior to establishing business relationships. New customers will be asked to complete an onboarding form and provide CDD documents as per the below, as supporting evidence.

Statutory Documents – Company

(Documents MUST be certified by a current acting director of the company)

- Company statutory documents
- Individual CDD for all Directors, beneficial owners who own more than 10% of the business and any other applicable authorised individuals (please see above for Proof of Address and Proof of Identity Documentation and certification requirements for individuals)
- Corporate Structure
- Bank statement must be in the name of the business registering and dated within 6 months and certified.

Proof of identity – Individual

(Document MUST be certified by a lawyer, notary, member of an accredited body (e.g. Certified Chartered accountant) or other public official.

- The requirement is that it must be a photo ID
- Must be in date

Any one of the following will be accepted as Proof of Identity;

Passport - This must be in date, a colour copy, and show both the photographic page and the opposing page clearly including all edges.

Driving License - We require only the front of the driving licence. This must be in date. If a driving licence is used as ID it cannot be used for Proof of Address.

National Identity Card - Both sides of the Card is required. The card must be in date.

Proof of Address – Individual

(Document MUST be certified by a lawyer, notary, member of an accredited body (e.g. Certified Chartered accountant) or other public official.

- The requirement is an official document that shows your residential address.
- Any document must be under 6 months old.

We are able to accept any one of the following as Proof of Address:

- **Utility Bill**
- **Driving License** (This cannot be used as ID if used here)
- **Bank Statement** (This should be a personal bank statement, in the name of the individual)

Further to the above, Sanction screening and PEP status screening will also be performed, where the said checks are to take place prior entering the business relationship.

The company will check published lists of known or suspected terrorists or other sanctioned persons or companies:

- EU sanction list
- U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons
- UN Sanction list

For the PEP status screening the company might rely on the combination of internal open-source checks and third party verification tools.

Customers that do not pass due diligence or are identified as a possible PEP or Sanctions listed individual will be subject to enhanced due diligence checks prior to having a business relationship established.

Enhanced due diligence will be conducted by a number of methods, including but is not limited to:

- Verification based on personal documents e.g. passport, identity card, proof of address, etc.
- Social media and publicly held data
- Privilege information from other operators, sources
- Financial or corporate data
- Third-party data providers

There is a higher risk of cryptocurrency being associated with Sanctions listed individuals who may be the subject of regulatory or financial sanctions, or resident in a country or jurisdiction which is a subject to financial, regulatory or other sanctions, limiting or restricting their use of the established financial and payments eco-systems.

As a result, Sanctions checks form a key aspect of the initial due diligence applied to new customers using crypto (digital) currency.

PEPs & SANCTIONS:

The definition of a Politically Exposed Person (PEP) in the National Ordinance on Identification when Rendering Services (NOIRS) is as follows:

Persons who hold or have a prominent public function with the exception of those who have held this position for less than a year, and the immediate family members or close associates of these persons.

In line with its obligations (Article 2 of NOIRS), the Company will:

a. Implement appropriate risk management systems to determine whether a client or ultimately interested party is politically vulnerable;

b. obtain approval from the persons responsible for the overall management of the service provider, for entering into a business relationship with or effecting a transaction for such client, or beneficial owner as well as obtaining such approval if during the business relationship the client or beneficial owner becomes a politically exposed person;

c. take risk-based and adequate measures to identify the source of political capacity prominent person and the funds used in the business relationship or transaction to pose; and

d. maintain on-going monitoring and tight control of the business relationship.

1. The following persons shall be persons performing prominent public functions, and subject to a PEP check:

a) a state, head of government, minister and deputy or assistant minister;

b) a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors, or of the board of a central bank;

c) an ambassador, a chargé d'affaires or a high-ranking officer in armed forces;

d) a member of an administrative, management or supervisory body of a State-owned enterprise.

e) a director, deputy director or member of the board, or equivalent function, of an international organization, except middle-ranking or more junior officials.

2. The following persons are considered family members of a person performing prominent public functions:

- a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or a local politically exposed person;
- b) a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;
- c) a parent of a politically exposed person or local politically exposed person.

3. The following persons are considered close associates of a person performing prominent public functions:

- a) a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a politically exposed person or a local politically exposed person;
- b) a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person or local politically exposed person.

Where a PEP is positively identified, the Company will conduct a full review and gain approval from the management board or service provider prior to establishing a business relationship.

The Company will conduct on-going PEP screening checks as part of its on-going due diligence procedures.

The following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

This means that the measures taken can be tailored to the risks in a specific case. Screening for PEP status shall be carried out before establishing the business relationship or conducting the occasional transaction.

The Company will ensure that it conducts appropriate due diligence checks to identify any individuals that may be subject to regulatory or financial sanctions or enforcements, known terrorists, money launderers, fraudsters and black-listed persons.

Where a Sanctions listed individual is positively identified the Company will not establish a business relationship but will conduct a review to establish is a disclosure should be submitted to law enforcement and notify the management board and/or service provider.

The Company will conduct on-going Sanctions screening checks as part of its on-going due diligence procedures.

ENHANCED DUE DILIGENCE

The Company shall conduct Enhanced Due Diligence procedures when a customer has been identified as high risk. Customers should be continually monitored by the Company for any update in their risk profile. Where behaviours or transactions are identified which may increase the Customer's potential risk, further investigations and due diligence should be undertaken. Factors which may increase a Customer's risk include suspicious activity, a match against a PEP/Sanctions list or a sudden change in behaviour, for example conducting transactions that are not in line with the customer's business objectives.

EDD measures include, but are not limited to, the following measures:

- Obtaining an additional method of photo ID
- Obtaining proof of source of funds/wealth (see below for acceptable documentation)
- Verifying client information with a reliable third party, ie Companies registry or other reputable third-party information provider

Source of Wealth Documents acceptable

The below is a list of examples of acceptable source of wealth documents, however this list is not exhaustive;

Savings from Salary (basic/or bonus)

- Original or certified copy of a payslip (or bonus payment)
- Letter from employer confirming salary
- Latest audited accounts and company bank statement

Sale of property

- Signed letter from solicitor
- Certified copy of sales contract
- Signed letter from estate agent

Sale of shares or other investments/liquidation of investment portfolio

- Certified Investment/savings certificates, contract notes or cash-in statements
- Bank statement clearly showing receipt of funds and investment company name

Inheritance

- Signed letter from solicitor
- Grant of probate (with a copy of the will), which must include the value of the estate

THE TERMINATION OF THE BUSINESS RELATIONSHIP

In the cases where the above due diligence onboarding requirements of this document cannot be met, the company shall not establish the business relationship with the customer. In those cases where the business relationship is already established, however there is a reasonable ground to for suspicion of any ML/FT/PF activity, the company might also terminate the business relationship with the customer. This action would be followed by appropriate report to the FIU. Termination of the business relationship might also occur in those scenarios where the customer is reluctant to provide the sufficient documentation to verify their identity.

In all the scenarios the company will document all the factors and information it has in its disposal as well as the steps taken in order to make the necessary documentation and information available.

ONGOING MONITORING:

The Company has a continuing duty to conduct ongoing monitoring of all customer relationships and to be vigilant with regard to money laundering and terrorist financing at all times and to report any suspicious transactions or circumstances.

The Company will monitor all customer transactions and activity in accordance with industry best practice, international recommendations and guidelines.

The conditions of ongoing monitoring such as frequency or the extent of the checks shall be determined by the risk level assigned during the stage of risk assessing the customer.

The Company will review any client who is classified as high risk every twelve months. All medium- and low-risk clients will be reviewed every two years. The review will ensure all due diligence information is still relevant and up to date. This includes:

- checking identification and address is still valid; if not, this will be updated
- checking there are no discrepancies on the person of significant control register
- checking annual turnover is in line with what we would expect.

Even if no changes are present, this will be documented and recorded.

Events prompting an immediate review include:

- a change in the client's identity
- a change in beneficial ownership of the client
- a change in the service provided to the client
- information that is inconsistent with the business's knowledge of the client.

7. REPORTING SUSPICIONS AND UNUSUAL TRANSACTIONS

The Company shall submit a formal suspicious activity report to law enforcement in respect of any individual that is positively identified as being on a Sanctions list, in accordance with the process set out in the Company's AML Policy.

In accordance with Article 1 of the National Ordinance on the Reporting of Unusual Transactions or NORUT (Landsverordening meldingongebruikelijke transacties (LMOT), PB 2017, no. 99) ('NORUT') the Company has a duty to report unusual (suspicious) transactions which may be linked to money laundering, the financing of terrorism or other criminal activity. This duty is also stated in Article 4 of the AML/CFT/CFP - Regulations released on May 20, 2024 by the Curacao Gaming Control Board.

The company is required to detect and report not only suspicious transactions, but also unusual transactions. This is achieved by having adequate procedures in place where the following areas are being covered:

1. The recognition of unusual transactions
2. The Documentation of unusual transactions
3. The reporting of unusual transactions

Where there are any concerns regarding any customer or any actual or attempted transaction, employees should in the first instance send an internal report to the Compliance Officer / Money Laundering Reporting Officer. The steps to making a formal report are as follows:

1. An internal suspicious transaction report must be made to the Compliance Officer / Money Laundering Reporting Officer no later than 24 hours between the execution of the transaction (or the intention to execute a transaction).
2. The Compliance Officer / Money Laundering Reporting Officer will have 10 working days to complete any additional investigations needed to ascertain the risk of money laundering, terrorist financing or other crime.
3. Following the period of investigation any unusual (suspicious) transaction report must be submitted within 48 hours of the Money Laundering Reporting Officer making the decision to submit a report.

If this is not possible the Company will submit a request for dispensation (5 days) in writing to the FIU, stating the reasons for the extension.

The Money Laundering Reporting Officer will also notify the management board and/or service provider that a formal report has been submitted.

SUBMITTING A FORMAL UNUSUAL (SUSPICIOUS) TRANSACTION REPORT

All reports must be submitted using the FIU online reporting system: FIU Curaçao and goAML reporting portal. All supporting documentation is to be included in such report and available in English.

The Company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. It is also not permitted to disclose information to the customer nor to third parties.

There are two types of indicators which are used to determine the type of report to be made:

1. Objective indicator - the circumstances under which a transaction is to be considered as unusual.
2. Subjective indicator - the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, and any other circumstance that may be relevant) has reasonable indications to presume that a transaction is related to money laundering or terrorism financing. For subjective indicators, red flags can be suggested by the supervisors and/or the FIU that indicate such possible presumptions.

The indicator letter for providers of Providers of Internet Gambling is: G

The indicators for internet (online) gaming and gambling operators are as shown below.

Objective indicators

<i>A. A transaction which is reported to the police or judicial authorities</i>	
Indicator	Definition
G0000111	A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
<i>B. An intended transaction carried out by or for the benefit of a natural person, legal person, group or entity which is on a list compiled by virtue of the Sanctions National Ordinance.</i>	
G0000114	An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
<i>C. A transaction amounting to NAF (ANG) 5,000.00 or more, regardless whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner; This comprises in any case the following situations:</i>	
G0000135	1. <i>A giro-based transaction amounting to NAF (ANG) 5,000.00 or more:</i> A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank account carried out at the request of the client addressed to the service provider.
	2. <i>The taking into deposit or the releasing out of deposit of an amount of NAF(ANG) 5,000.00 or more, at the request of the client.</i>
	3. <i>Sale of tokens to a client in the amount of NAF (ANG) 5,000.00 or more.</i> The term "tokens" includes at least chips and credits.
	4. <i>Payout of prizes in the amount of NAF (ANG) 5.000,-- or more.</i>
	5. <i>All other cases.</i>
NB In case of Indicator G0000135: please also indicate the applicable sub-indicator (1,2,3,4 or 5) when reporting a transaction. In case of sub-indicator 5, please always provide a description of the situation.	

Subjective indicator

<i>Suspected money laundering transactions or financing of terrorism.</i>	
Indicator	Definition`
G0000211	A transaction giving cause to assume that it may be connected with money laundering or terrorist financing.

8. RECORD-KEEPING

The Compliance Officer / Money Laundering Reporting Officer will maintain a full record of and notify the management board and/or the service provider of the following:

- all internal reports received;
- review and decision-making process;
- all formal unusual (suspicious) transaction reports made to the FIU
- all individuals that are identified as a PEP
- all individuals that are identified as a possible Sanctions listed individual and the outcome of any review of that individual

The Company shall store and maintain for a period of minimum 5 years all necessary records on transactions. All records obtained through Due Diligence measures (such as ID cards, driving licenses, passports, and more) shall be also kept for a minimum period of 5 years since the date of the last occasional transaction or since the day due to which the business relationship with the customer has ended.

9. ANTI-MONEY LAUNDERING PROGRAM

INTRODUCTION

An anti-money laundering program is an essential component of the Company compliance regime. The primary goal of the program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations.

The core elements the Anti-Money Laundering Compliance Program is addressing, are:

1. A system of internal policies, procedures and controls;
2. A designated compliance officer with day-to-day oversight over the AML program;
3. An employee screening program and ongoing employee training program; and
4. An independent audit function to test the AML program.

The Company tests the anti-money laundering program systematically and adapts the program to the current risks that arise within the Company's own organization. The AML program has the approval of senior management.

INTERNAL POLICIES, PROCEDURES AND CONTROLS

The Company is committed to combat any possible abuse of its facilities, products and services for purpose of Money Laundering, Terrorist Financing and the Proliferation Financing. For this purpose, the Company puts in place specifically designed policies, procedures and controls which are being periodically revisited to ensure their ongoing efficiency of their design.

This policy is in place as the master policy of the Company for AML/CTF/PF areas, where further details on practices and guidelines are included in the Companies' AML/CFT/PF procedures and internal controls. All policies, procedures and controls are reviewed and approved by senior management or the board of directors.

THE APPOINTMENT OF A COMPLIANCE OFFICER

The Company shall formally designate a senior officer at management level and independent from the game's operations, responsible for the detection and deterrence of money laundering and terrorist financing. The Company will also ensure that the designated individual has sufficient experience, time and resources in order to perform this role and its responsibilities.

The duties of the Compliance Officer are, but not limited to:

- To design, implement and maintain the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the Company's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;

The above-mentioned responsibilities shall be included in the job description of the compliance officer. The job description shall be signed off and dated by the officer, indicating his/her acceptance of the entrusted responsibilities.

The current Compliance Officer is: Angeline Hassan

Name: Angeline Chen Hassan

Contact details: Angeline@casterbridgepartners.com

THE EMPLOYEE SCREENING AND ONGOING TRAINING PROGRAM

All new employees are subject to screening for criminal background and designated procedures are in place for the onboarding process. The Company also has a training program in place for its both new and current staff. All employees are receiving training / re-training based on their role designation and the time period passed since the initial training.

All new employees, irrespective of their level of seniority, shall received the training of the nature and process of Money Laundering and Terrorist financing. This also extends to any and all the Company's audit staff, AML Compliance staff, supervisors and managers, senior managers and the board of directors.

Following records shall be also kept at all times in the designated training register:

- Details on the content of the training programs;
- The names of the staff members who have received the training;
- The date on which the training was provided;
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and
- An ongoing training plan.

AN INDEPENDENT AUDIT FUNCTION

An independent audit is being performed on the Company's AML Compliance Program on annual basis, to test the robustness and efficiency if the AML policies, procedures and controls. The audit is performed by the Company's independent internal audit team.

The sets of tests shall include, but not be limited to:

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

Internal Audit Director is:

Name: Daniel Howard

Contact: danny@casterbridgepartners.com

The scope of the testing and the testing results shall be documented, with any deficiencies reported to senior management and/or the Board of Supervisory Directors, and to the designated officers with a request to take prompt corrective actions by a certain deadline.

10. Restricted Jurisdictions

- Curaçao
- Netherlands
- France
- Spain
- Belgium
- Germany
- Lithuania
- USA
- UK
- Australia
- Estonia
- Afghanistan
- North Korea
- Iran
- Syria
- Yemen
- Serbia
- Myanmar
- Ukraine
- Portugal
- Russia
- Any other prohibited jurisdiction, jurisdiction on sanction lists, jurisdictions that deems online gambling illegal or blacklisted according to market and regulatory developments

Document Name: AML/CFT Manual – AML/CFT Policy and Procedures v1.0

Authorized By:

Updated By:

Author:

Date:

Signed: