

Pomadorro N.V.

**RULES FOR THE ANTI-MONEY LAUDERING AND COUNTER-
TERRORIST FINANCING AND COUNTER-PROLIFERATION
FINANCING**

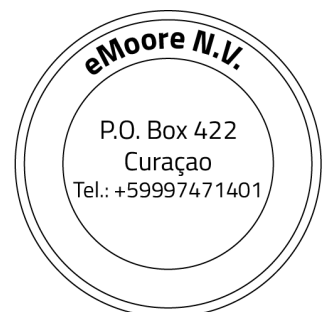
Version 1.3.

2024

Deeuw

16/04/2024

Executed by C. van der Leeuw as Proxy Holder eMoore NV



INTRODUCTION	3
DEFINITIONS	3
1. Company Policy	5
2. Objective of the Policy	6
3. Regulatory Framework.....	6
4. Player Research	8
5. Player identification, research and transaction monitoring program	8
6. Risk-Based Customer Due Diligence And Risk Profiling	14
7. Continuous transaction due diligence.....	15
8. Suspicious Transactions and Reporting	18
9. Documentation storage.....	19
10. Training Programs	19
11. Staff Due Diligence	20
12. Independent Testing Of The AML Policy	20

INTRODUCTION

The Money Laundering and any Activity that Facilitates Money Laundering or the Funding of Terrorist or Criminal Activities and Sanctions Risk Management Policy (hereinafter - the Policy) of Pomadorro N.V. (also hereinafter referred to as the “Company”) is developed based on requirements of the applicable normative acts of the Curacao and on generally accepted standards of international practice.

This Policy describes in more detail the measures, actions and procedures that Pomadorro N.V. must perform in accordance with the laws and the regulatory requirements of Curacao and the countries in which Pomadorro N.V. operates (hereinafter referred to as the “Rules”) in order to detect and prevent attempts to launder money and finance terrorism. The Company implements the Policy through the creation of an effective system to prevent money laundering and terrorist financing.

The Company is obliged to implement, constantly update the Policy in accordance with the Rules and Recommendations and other provisions that regulate the system of prevention of money laundering and financing of terrorism. All employees and subdivisions of Pomadorro N.V. are required to implement this Policy.

DEFINITIONS

Money laundering - is the process by which criminal proceeds are "cleaned" so that their illegal origins are hidden. It is usually associated with the types of organized crime that generate huge profits in cash, such as trafficking in drugs, weapons and human beings as well as fraud. Although it is not possible to measure money laundering in the same way as legitimate economic activity, the scale of the problem is considered to be enormous. Examples of such actions can be: conversion or transfer of property acquired from criminal activity, with aim to conceal or disguise its origin, or to assist a person committing criminal activity to evade the legal consequences of this person's actions, conceal or disguise real origin of a source, place, movement of a property or handling or modification of rights with respect to a property, knowing that such a property was acquired from criminal activity. acquisition, possession, use or disposal of property, being aware of its origin from criminal activity. in a criminal confederacy of persons or other types of collaboration for actions stated above. Terrorist

financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Politically exposed person - means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons. Politically exposed person includes the following:

- heads of State, heads of government, ministers and deputy or assistant ministers;
- members of parliament or of similar legislative bodies;
- 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 not subject to further appeal, except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, chargés d'affaires and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned enterprises;
- directors, deputy directors and members of the board or equivalent function of an international organization.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials;

Family members includes the following:

- the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
- the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
- the parents of a politically exposed person;

Persons known to be close associates' means:

- natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
- natural persons who have 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.

Player - a natural person to which the Company provides a service

Suspicious transaction – transaction carried out under circumstances suspicious of money laundering or terrorism financing, or circumstances suggesting that the transaction is in any other way linked to terrorism financing, or any fact that could lead to such a suspicion. Suspicious circumstances can be e.g. abnormalities in user’s behavior contrary to his usual behavior or contrary to behavior of similar type of users.

1. Company Policy

1.1. This Policy of the Company is meant to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities (also hereinafter to as the “Policy”). The Company strives to comply with all applicable requirements under the legislations in force in the jurisdictions of the European Union members in which the Company operates, pursuant to the *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*¹ and the forthcoming Fourth Directive on Money laundering.

1.2. The Company is licensed and regulated by Curacao. The main business of the Company is to offer remote (on-line) games over the Internet, under the National Decree August 18, 1998 No. 14. Under the license conditions issued by Curaçao, the Company is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

¹ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance). Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060>

1.3. The Company is therefore obliged to follow the provisions contained in the Curaçao legal framework in particular the National Decree August 18, 1998 No. 14 and the legislations in force in any other jurisdiction in which the Company undertakes its activities.

2. Objective of the Policy

2.1. The Company is fully committed to be constantly vigilant to prevent money laundering and combat the financing of terrorism in order to minimize and manage risks such as reputational risk, legal risk and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes.

2.2. The Company endeavor to keep itself updated with developments both at national and international level on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorist and other criminal activities.

2.3. The Company's policies, procedures and internal controls are designed to ensure compliance with all applicable laws, rules, directives and regulations relevant to the Company's operations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place.

3. Regulatory Framework

3.1 Pursuant to the National Ordinance of Money Laundering (1993), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

- a) The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

c) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

d) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);

e) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);

f) National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

3.2 As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting International standards by regularly implementing these standards in its national legislation. On international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally. In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF. Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

4. Player Research

4.1. When Player research measures are to be Performed:

The Company shall perform player research measures in accordance with this Policy when –

- (a) a player makes a deposit or obtains a refund, a reward or a win;
- (b) there is a suspicion of money laundering, terrorist financing and proliferation financing or an attempt to commit such activities;
- (c) The Company has doubts about the veracity or adequacy of any information previously obtained;
- (d) the player is a politically significant person, a member of the family of a politically significant person or a person closely associated with a politically significant person.

4.2. If an employee of the Company has not noticed 3.1. (a, b, c, d), the customer survey doesn't have to be performed.

4.3. The overarching goal of the client's investigation is to obtain assurance that the funds involved in the transaction have not been obtained by criminal means, the purpose of the transaction is not related to such money laundering attempts or the transaction funds will not be used to finance terrorism or proliferation.

4.4. In order to implement the overarching goal referred to in Clause 3.3., the main goal of the client's research is to determine the client's risk in connection with the possibility of money laundering or terrorist or proliferation financing.

5. Player identification, research and transaction monitoring program

5.1. The Company will take reasonable steps to establish the identity of any person for whom it is proposed to provide its service (hereinafter "Players"). The registration process is a comprehensive verification procedure, which must be carried out before the player's profile is opened; it is described in the general terms and conditions of the Company and below.

5.2. The Company will keep at all times a secure list of all registered Players and information and documents will be retained in accordance with the applicable data protection obligations.

5.3. The Company will collect certain identification information from each Player who opens an account. The Company will not open anonymous accounts or accounts in fictitious names so that the true beneficial owner is not known. The information required will include at least:

- a. Player's date of birth (showing that the player is over eighteen (18) years of age);
- b. Player's first and last name;
- c. Player's place of residence;
- d. Player's credit card or banking information;
- e. Player's valid email address; and
- f. Player's username and a password.

5.4. On registration, a geographical location check is carried out on the Player's computer IP to ensure that person is in a permitted jurisdiction. If the Player is not in a permitted jurisdiction, he/she will not be allowed to continue the registration process.

5.5. When the Company deals with any request for a relevant transaction, the Company shall review the earlier relevant transactions (if any) undertaken by the Player concerned to ensure that the current transaction is consistent with his knowledge of the user. The Company shall pay special attention to all complex or unusually large relevant transactions or unusual patterns of relevant transactions, that have no apparent economic or lawful purpose. Documents to verify the identity information received will be requested from the Player if and when there is considered to be risk or uncertainty about the information provided. These documents shall include, to the extent permitted under the relevant data protection regulations:

- a. A copy of a valid identity card or passport;
- b. Proof of address;

5.6. The Company may supplement the use of documentary evidence by using other means which may include:

- a. Independently verifying the Player's identity through the comparison of information provided by the Player with information obtained from a reporting agency, public database or other source;
- b. Checking references with financial institutions; or
- c. Obtaining a financial statement.

5.7. The Company will inform relevant Players that the Company may seek identification information to verify their identity, and will compare Player identification information with government or international lists of suspected terrorists or sanction lists for example through the European Union or FATF on a monthly basis.

5.8. Any employee of the Company who becomes aware of an uncertainty in relation to the accuracy and truthfulness of the Player information provided shall immediately notify the responsible employee, who will review the materials and determine whether further identification is required and or so that it may be determined whether a report is to be sent to the FIU of Curaçao. In case a report is filed with the FIU or any internal investigation is taking place, it is prohibited to inform the Player thereof, let alone divulge details of such transaction (prohibition of tipping-off).

5.9. Upon the suspicion of the multiple registration by Players acting in collusion or as a syndicate, the set-up of fictitious accounts or the use of front men, the Company reserves the right to change or terminate any bonus offer, cancel any winnings and close accounts.

5.10. If a potential or existing Player either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, the AML responsible employee will be notified so that it may be determined whether a report is to be sent to the FIU of Curaçao.

5.11. If a Player appears on a list of suspected terrorists or otherwise sanctioned individuals the Company will take the appropriate steps to immediately freeze and or lose the account of the Player.

5.12. If any significant personal information of a Player changes, verification documents will be requested.

5.13. If the player is a politically exposed person, a relative or a person closely associated with the politically exposed person:

- must obtain permission from senior management to enter into or continue a business relationship;
- all risk-based procedures that identify the source of funds and material well-being of the client must be documented.

5.14. Verification and Validation of Identity Information

In accordance with the laws and regulations mentioned in Clause 3.1., the content of information as is collected may vary, and in principle, the following information should be collected for an individual account:

- name;
- address (and permanent address, if the two are different);
- date of birth;
- nationality;
- place of issuance of the identification document;
- validity of the identification document.

The following documents are accepted as the identity proof:

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

The identification documents are only accepted in English language. In cases when the document is issued in other languages – a certified translation is required.

The identification documents are only accepted in high quality as a scan, photocopy or a photograph; all four corners of the document should be visible, and in case of ID cards – both sides should be provided.

The document should not be accepted in the following cases:

- When it is difficult to read the information in the identification documents due to poor quality;
- When it is difficult to see the photo of the identification document holder due to poor quality;
- When some information and/or part of the document is covered or for any other reason cannot be seen;

- When only a certain part of the identification document is received;
- When the identification document is received in other language than English and cannot be read.

The following documents are accepted as the proof of address:

- correspondence from a central or local government authority, department or agency;
- an official conduct certificate;
- any other government-issued document not mentioned above;
- a lease contract or agreement;
- Utility bill (gas/electricity/home internet) – not older than 3 months;
- a bank statement or a reference letter issued by a recognised credit institution or entity – not older than 3 months.

The document should not be accepted in the following cases:

- When the received document is older than 3 months;
- When it is difficult to read the information in the identification documents due to poor quality;
- When some information and/or part of the document is covered or for any other reason cannot be seen;
- When the document is received in other language than English and cannot be read;
- When the name on the proof of address does not match the name in the identification document.

In cases when the inappropriate or insufficient document is received – another copy and/or document should be received in order to complete the verification procedure.

5.15. Verification and Validation of Source of Funds

Source of Funds validation and verification should be conducted for ongoing monitoring purposes, as well as with respect to politically exposed persons (PEPs).

Enhanced due diligence and enhanced ongoing monitoring should be carried on when:

- a high risk of money laundering has been identified under the risk assessment or from information provided;
- player is from a high-risk third country;
- the Player is a PEP;

- any other situation which can be assessed as presenting a higher risk of money laundering;
- the transaction:
 - is complex;
 - unusually large;
 - forms an unusual pattern of transactions;
 - has no apparent economic or legal purpose.

As part of the EDD process, the source of wealth should be verified with evidence obtained from the Player and/or independent source until it is understandable where the Player's overall wealth has been derived from and (to the best of knowledge) that it's legitimate.

The type of documentation acceptable to verifying source of funds depends on the level of risk.

If the transaction is higher risk, you may ask for supporting evidence, possibly in the form of:

- bank statements;
- recently filed personal income accounts;
- documents confirming the source, such as:
 - sale of a house;
 - sale of shares;
 - receipt of a personal injuries award;
 - a bequest under an estate;
 - a win from gambling activities etc.

Where cash is involved, it becomes more challenging. A bank statement showing a large withdrawal does not mean that the cash the Player is now in possession of was actually the money withdrawn. Equally, a bank statement showing a large cash deposit does not provide information about where the cash came from in the first place.

5.16. PEP (Politically Exposed Persons) and Sanctions Screening

All Players, upon registration, are screened against all sanctions list and existing PEP lists. Re-screening is also conducted on regular basis.

For PEPs, family members, close associate and entities in which their presence is founded, an enhanced due diligence must be conducted:

- have approval from the responsible employee or senior management for establishing or continuing the business relationship with that person;
- where the business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with that Customer.

5.17. Sanctions

Any potential matches are immediately reviewed and verified prior to onboarding if confirmed as false matches. If a true match is detected, the onboarding is rejected, and the relationship is exited. Further actions (such as reporting to the authorities) may be taken on case by case basis and if required. The Company complies with the following sanctions measures:

- The United Nations (UN) Security Council consolidated sanctions list;
- The EU's consolidated list of persons, groups and entities;
- The UK HM Treasury (HMT), Office of Financial Sanctions Implementation, "consolidated list of targets"
- The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists including the SDN list (Specially Designated Nationals and Blocked Persons List);
- Any local government issued list.

6. Risk-Based Customer Due Diligence And Risk Profiling

Risk of all the Players shall be categorized into 3 different categories: High Risk, Medium Risk and Low Risk based on their risk profile considering certain indicative criteria to avoid money laundering and other compliance risk.

6.1. Low Risk: Players whose identities and sources of wealth can be easily identified and transaction maintained by such customer is done via bank account shall be categorized as "Low Risk".

6.2. Medium Risk: Players who are conducting normal nature of wealth but lack sufficient information and documents for categorizing under 'Low Risk' shall normally be categorized as medium risk. Besides, all Players who do not fall under the category of either High Risk or Low Risk profile shall also be categorized as Medium risk.

6.3. High Risk: Players that are likely to pose a higher risk depending on their background, sources of funds etc. can be categorized as high risk. Also as High Risk Players should be categorized Players, who make payments using cryptocurrencies.

Some of the indicative list of High Risk Clients are:

- Players having unusual amount of transactions.
- Players willing to use withdrawal methods different to methods used for deposit.
- Any related person who is suspected for directly or indirectly assisting terrorism, terrorist activities, terrorist organizations, organized crimes, illicit drugs and any other criminal activities. Normally the Company should not establish business relationship with such Clients.
- Players who have been generally known through public media to be involved in Money Laundering and other financial crimes.
- Players, who have been understood / heard to be involved in evading or misappropriating tax, customs, fees or any other revenue.
- Players are residents of the country, which is classified as non-cooperative country by Financial Action Task Force (FATF).
- Players are citizens of a country on which the United Nations or any Inter Governmental International Organizations has imposed sanctions or warns.
- Players are connected to the PEP.

7. Continuous transaction due diligence

7.1. The Company will monitor account activity with special attention, and to the extent possible, the background and purpose of any more complex or large transactions and any transactions which are particularly likely, by their nature, to be related to money laundering or the funding of terrorism.

7.2. Monitoring will be conducted through the following methods: Transactions will be automatically monitored and a report will be generated daily that show all transactions above 3,000 EURO along with all the details of the users making those transactions. An additional report will be generated daily per user that made a transaction above 3,000 EURO detailing their collected ID documents, collected personal details, and their entire account transaction history.

7.3. The employee, responsible for this monitoring, will review any activity that the monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the FIU of Curaçao.

7.4. Parameters that signal possible money laundering or terrorist financing include, but are not limited to:

7.4.1. Wire transfers to/from financial secrecy havens or high-risk geographic location/ jurisdiction without an apparent reason.

High-risk third countries that have expressed a high-level political commitment to address the identified shortcomings and have decided to request technical assistance in the implementation of the FATF Action Plan:

- Iran

High-risk third countries that have repeatedly failed to address the identified shortcomings and thus pose a persistent and significant risk of money laundering and terrorist financing:

- Democratic People's Republic of Korea (DPRK)

FATF high-risk third countries that have expressed a political commitment to address the identified shortcomings and have developed an action plan in cooperation with the FATF:

Albania	Haiti	South Africa
Barbados	Jamaica	South Sudan
Bulgaria	Jordan	Syria
Burkina Faso	Mali	Tanzania
Cameroon	Mozambique	Türkiye
Cayman Islands	Nigeria	Uganda
Democratic Republic of Congo	Panama	United Arab Emirates
Croatia	Philippines	Vietnam
Gibraltar	Senegal	Yemen

7.4.2. The Company forbids accounts to be opened by, or make any deposits nor used from, customers who are residents (or citizens) of the following countries:

Australia	Germany	Macau	Sweden
Belgium	Hong Kong	Netherlands	Switzerland
Czech Republic	Hungary	Portugal	Taiwan
Denmark	Italy	Russia	Ukraine
Estonia	Latvia	Slovakia	United Kingdom
France	Lithuania	Spain	United States of America

7.4.3. The Company forbids accounts to be opened by, or make any deposits nor used from, customers who are residents (or citizens) of countries or territories against which international sanctions are imposed, as well as countries or territories with limited international recognition.

7.4.4. Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out.

7.4.5. Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent specific purpose.

7.5. The following can be considered as risk mitigating factors in player research and transaction monitoring:

- a country with an effective anti-money laundering and anti-terrorist financing system;
- a country that applies international anti-money laundering and anti-terrorist financing standards;
- a country with a low risk of corruption;
- a country with a low proportion of crimes that generate criminal resources.

7.6. When an employee of the Company detects any activity that may be suspicious, he or she will notify the responsible employee. Responsible employee will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or filing a report.

7.7. The Company will not accept cash or non-electronic payments from Players. Funds may be received from Players only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer cheques and any other method approved by the respective regulators.

7.8. The Company will only transfer payments of winnings or refunds back to the same route from where the funds originated, where possible.

7.9. Transfers of funds between Players accounts are prohibited.

7.10. To the extent the Company utilizes a third party to process and record payments to and from Player and accounts, the Company will ensure the services provider has transaction monitoring systems in place which will allow for screening of the transactions pursuant to these provisions and in accordance with the applicable legislation. The responsible employee shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

7.11. Records relating to the financial transactions shall be maintained in accordance with the data protection and retention requirements in the applicable jurisdiction of Curaçao.

8. Suspicious Transactions and Reporting

The responsible employee will report any suspicious transactions (including deposits and transfers) conducted or attempted by, at or through a Player account involving EUR 3,000 or more of funds (either individually or in the aggregate) where the responsible employee knows, suspects or has reason to suspect:

- a. The Player is included on any list of individuals assumed associated with terrorism or on a sanctions list;
- b. The Player is politically exposed person;
- c. The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations or to avoid any transaction reporting requirement under law or regulation;
- d. The transaction has no ordinary lawful purpose or is not the sort in which the Player would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
- e. The transaction involves the use of the Company to facilitate criminal activity.

9. Documentation storage

9.1. For at least five years after the termination of the business relationship or the performance of an incidental transaction, the company keeps:

- all information obtained within the framework of the player research, including information about the player and his accounts, copies of documents certifying the player's identification data, the results of the player's research;
- information on all payments made by the player and winnings;
- correspondence with the player, including electronic correspondence.

9.2. At the end of the storage period, the Company destroys the documents and personal information in its possession. The period of storage of player information begins after the termination of the business relationship.

9.3. If a player has established a business relationship and does not subsequently maintain it, such business relationship must be considered as existing.

10. Training Programs

10.1. The Company ensures that its employees are adequately trained and informed about the requirements set out in Company's AML/CTF and Sanctions policies and procedures. The Company also ensures that the daily duties of its employees are executed in accordance with Company's regulations and technical instructions specified in Company's AML/CTF and Sanctions procedures. An employee of the Company, who violates AML/CTF regulatory documents or acts illegally in the course of performance of his/her duties, shall be subject to disciplinary sanctions, as stipulated in Company's rules of internal order, and to the liability, as provided for in the regulatory enactments of the Curacao.

10.2. Employee AML/CTF and Sanctions training is comprised of two key elements:

10.2.1. Induction Training – the responsible employee is responsible for identifying relevant new staff that are required to undertake induction training within 45 days after commencement of employment relationship. The training is provided by the responsible employee or an external service provider and is a face to face training. The contents of the training include awareness training, covering ML/TF and

Sanctions. Until a new member of staff has been signed off as competent, no direct client contact is allowed;

10.2.2. Refresh Training - all relevant staff must undertake a face to face refresher or online training at least an annual basis. The training is provided by the responsible employee or an external service provider, and assessment of staff understanding is carried out throughout the training.

The training includes also:

10.2.3. how to identify red flags and signs of money laundering that arise during the course of the employees' duties;

10.2.4. what to do once the risk is identified (including how, when and to whom to escalate unusual Player activity or other red flags for analysis;

10.2.5. what employees' roles are in the Company's compliance efforts and how to perform them;

10.2.6. the Company's record retention policy; and

10.2.7. the disciplinary consequences for non-compliance with legislation.

10.3. The Company develop ongoing employee training under the leadership of the responsible employee and senior management. The training occurs on at least an annual basis. It based on the Company's size, its Player base, and its resources and be updated as necessary to reflect any new developments in the law.

11. Staff Due Diligence

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates, which are checked and verified by the Company's Human Resources Department.

12. Independent Testing Of The AML Policy

The independent audit assesses the level of money laundering risk for Company and should provide a fair and unbiased opinion of the Anti-Money Laundering compliance program.

To maintain independence, anyone who participates in AML testing is not permitted to be involved in establishing or performing ongoing AML compliance processes. This rule applies both to staff members and to any external party.

Auditors completing the test plan should report directly to the Managing Directors.

The Company should conduct independent testing every 12 to 18 months, or more often if required by a risk profile. An acquisition or a money laundering incident, for example, could trigger the need for more frequent testing.

Qualification requirements extend to both those carrying out internally executed test plans and those conducting outsourced test plans. Testing should be executed and supervised by people with expertise in the subject matter, auditing requirements, and institution type. Experience with specific AML systems or models is also a primary consideration when determining an individual's qualifications. Examiners consider not only an individual's audit experience but also professional credentials.

Reports on independent testing should be a basis for regular revise and update of this Policy

Date: March 4, 2024