

ALISIUM B.V.

**Anti-Money Laundering and Counter Terrorism Financing and Proliferation
of weapons of mass destruction Policy and Procedures**

Table of Contents

1. Version Control	4
2. Terms and Abbreviations	5
3. Company Policy Statement	7
4. Objective of the Policy	7
5. Regulatory Framework	8
6. Role of Compliance	9
7. Definition of money laundering	9
8. What is Terrorism Financing?	11
9. What is Proliferation of Weapons of Mass Destruction	12
10. Client Acceptance Policy	13
11. Risk Management and Client Risk Assessment	13
12. Customer Due Diligence	15
13. Simplified Due Diligence Rules	19
14. CDD and On-Going Monitoring Process Record Keeping	19
15. Correspondence with the Client	20
16. Document Translation and Certification	20
17. Acceptable Identity Verification Documents	20
18. Acceptable address confirmation documents	21
19. Enhanced Due Diligence	21
20. EDD during the course of business relationship	22
21. On-going monitoring	24
22. Periodic review	26
23. Crypto Usage Policy	27
24. Politically Exposed Persons	28
25. Sanctions	29
26. Dealing with sanctioned persons	31
27. Termination of the business relationship	31
28. Compliance Officer	32
29. Reporting Requirements	34
30. Reporting Procedure: Internal reporting	36
31. Reporting Procedure: External reporting	37
32. Dealing with the requests from the Authorities	37
33. Tipping Off	38
34. Training	39
35. Staff recruitment	40
36. Staff Responsibilities	40
37. Record Keeping	41
38. Funds Management procedure and Pay-out of gambling winnings	42
39. Fictitious, Anonymous & Multiple Accounts (fraud management)	43

40. Reliance on Third Parties	44
41. Business Risk Assessment	44
42. Technological Developments Risk Assessment	45
43. Internal Controls and Compliance	45
44. AML Compliance Program	46
45. Policy Breaches And Disciplinary Actions	47
46. Policy Revision	47
47. Annex 1: Indicators of Suspicious Activity of Money Laundering / Terrorist Financing	48
48. Annex 2: Examples of documents, that can prove client's source of funds/wealth	50
49. Annex 4: KYC questionnaire for natural persons	54
50. Annex 5: List of links to public registers	55
51. Annex 6: Internal Unusual Transaction Report	56

1. Version Control

Name	Description
Document Name	Anti-Money Laundering and Counter Terrorism Financing and Proliferation of weapons of mass destruction Policy and Procedures
Version	1.2
Owner/Responsible department	Compliance Department
Authorised By	Board of Directors
Latest Distribution and Effective Date	12.12.2025
Next Review Date	20.12.2026

Version	Description	Date	Initials
1.0	Policy update	15.05.2023	
1.1	Policy review and update	01.05.2024	
1.2	Policy review and update	20.03.2025	
1.3	Policy review and update	12.12.2025	

2. Terms and Abbreviations

AML – Anti-Money Laundering

XCG - Caribbean Guilders

CDD – Customer Due Diligence

CFT – Combating of Terrorism Financing

CGA - Curacao Gaming Authority

CO - Compliance Officer

CPF - Combating Financing of Proliferation of Weapons of Mass Destruction

EDD – Enhanced Due Diligence

FIU – Financial Intelligence Unit (Curacao)

KYC – Know Your Client

ML/FT/PF – Money Laundering / Funding of Terrorism / Financing Proliferation of Weapons of Mass Destruction

PEP – Politically Exposed Person

NORUT – National Ordinance Reporting Unusual Transactions

NOIS - National Ordinance Identification when Rendering Services

UTR - Unusual Transaction Report

WMD - Weapons of Mass Destruction

The Company – Alisium B.V., a limited liability company established under the laws of Curaçao, registered with the Chamber of Commerce of Curaçao under number 161507

The System – the Company’s core operating system Fundist

Business relationship – a business professional or commercial relationship between the Company and the Client which is expected by the Company, at the time when contact is established, to have an element of duration;

Client - Private individual, who completes the registration and identification process, enabling him to make use of the online gaming services on the Websites; thus, a private individual, who has a business relationship with and uses the services provided by the Company, based on the concluded servicing agreement (Terms of Use).

Client Profile - Aggregate of data and documents kept by the Company on its Clients, the Clients’ business/personal activities and transactions and any other information relevant for the Clients’ risk management

(incl. ID documents, data obtained from public sources of information, documents on source of funds (SoF), source of wealth (SoW), etc.).

Compliance Officer - the senior employee of the Company, who is in charge of the AML/CFT/CPF compliance department of the Company and whose detailed responsibilities are described in Section 28 of this Policy.

Employee - A duly authorized employee of the AML department, who evaluates the information obtained from the Client, performs Customer Due Diligence, Risk Scoring, Clients' on-going monitoring, and other functions as described in the Employee's job description with respect to ML/FT and Sanctions risk management.

Foundation means a foundation, wherever established;

Introducer means a person who has a Business Relationship with a Legal Person and who introduces that Legal Person to the Company with the intention that the Legal Person will form a Business Relationship or conduct an Occasional Transaction with the Company so that the Legal Person becomes a Partner of the Company;

KYC Questionnaire - Information about the Client obtained during the Customer Due Diligence process, which the Clients submit via the website. The obtained information is stored in the Client Profile and used for AML/CFT and Sanctions risk assessment. The information includes personal data, personal activity, source of funds, expected nature of business relationship, etc.

Legal Person includes a company, a partnership, whether limited or general, an association or any unincorporated body of persons, but does not include a trust;

Partner means any Legal Person with whom the Company has or expects to establish a Business Relationship or Occasional Transaction;

PEP - politically exposed person - natural person who is or has been entrusted with prominent public functions in or outside Curacao, such as but not limited to Heads of State / Government, Ministers, Deputy or Assistant Ministers, Parliamentary Secretaries, Members of Court, Ambassadors, Members of the administrative, management or supervisory boards of State-owned enterprises (other than middle ranking or more junior officials).

Domestic Politically Exposed Person means a person who is or has been entrusted with a prominent public function by the State;

Foreign Politically Exposed Person means a person who is, or has been entrusted with a prominent function by an international organization;

Regulations means the Anti-Money Laundering and Combating Terrorism Financing and Proliferation of Weapons of Mass Destruction Regulations applicable to business activity of the Company and/or any relevant regulatory or governmental obligations;

Source of Funds refers to the origin of the particular funds that are involved in a particular transaction. Annex 2 to this Policy lists possible examples of source of funds.

Source of Wealth is distinct from Source of Funds and comprises the full net worth of an individual. This is to ensure that the Company fully understands who the Client is, how he can afford certain deposits into his wallet, and what activity has generated the funds. Therefore, the Client may declare the source of his wealth has come from multiple categories;

Sumsb - Sum & Substance Ltd., the AML screening provider used by the Company to comply with its PEP and Sanctions screening obligations.

UBO - Ultimate Beneficial Owner - means any natural person(s), who ultimately own or control the Client and, or the natural person(s) on whose behalf a transaction or activity is being conducted. In case of body corporate, any individual who ultimately owns or controls (in each case whether directly or indirectly), more than 25% of the shares or voting rights in the body corporate, or any individual who exercises ultimate control over the body corporate or the management of the body corporate.

Websites means all websites authorized under a valid gaming license in the name of the Company, which can be accessed by means of a domain name and where Clients can access the online gaming services.

3. Company Policy Statement

It is the policy of the Company to strictly prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorism, proliferation of weapons of mass destruction or criminal activities. The Company strives to comply with all applicable requirements under the legislation in force in the jurisdictions in which the Company operates, including Curacao AML/CFT/CPF laws and regulations, to prevent the use of the financial system for the purpose of money laundering, terrorism financing or proliferation of weapons of mass destruction.

The Company is incorporated in Curacao and is licensed and regulated by the Curacao Gaming Authority to offer remote games of chance over the internet, under the license conditions issued by the CGA. The Company is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, financing of terrorism and proliferation of weapons of mass destruction or any other criminal activity.

4. Objective of the Policy

1. It is the policy of the Company to comply in all respects with the requirements of the Anti-Money Laundering Legislation by ensuring that the Company has policies and procedures to aid compliance.
2. The main scope of this policy is to establish the essential standards designed to prevent the Company from being used for money laundering, financing of terrorism and proliferation of weapons of mass destruction or any other criminal activity. This AML/CFT/CPF policy applies to the Company and all of its staff, whether on a full or part time basis, and to any subcontractor and its staff who provide services which might be used to conceal or disguise the true origins of criminally derived proceeds with the intention to make unlawful proceeds appear to have derived from legitimate origins or to constitute legitimate assets.
3. The Company is fully committed to be constantly vigilant to prevent money laundering, combat the financing of terrorism and proliferation of weapons of mass destruction in order to minimize and manage risks such as the reputational risk, legal risk and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its services to be abused in furtherance of these crimes.
4. The Company will endeavor to keep itself updated with developments both at national and international level on any initiatives to prevent money laundering, the financing of terrorism, proliferation of weapons of mass destruction. It commits itself to protect, at all times, the Company and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorism, proliferation of weapons of mass destruction and other criminal activities.
5. 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. Ongoing monitoring and compliance tests will take place to provide assurance to the Board and the regulators that The Company continues to meet its obligations under AML/CFT/CPF legislation.

5. Regulatory Framework

National regulations

The following main national regulations relating to money laundering, terrorist financing and proliferation of weapons of mass destruction are applicable to the Company:

- a) The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- b) The National Ordinance on Identification of Clients when Rendering Services (NOIS) (N.G. 2017, no. 92), as amended on May 16th, 2024 together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c) The National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), as amended on May 16th, 2024 together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d) Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- e) Sanctions National Ordinance (N.G. 2014, no. 55);
- f) Kingdom Sanction Act (N.G. 2016, no. 54);
- g) National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- h) National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- i) National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- j) National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- k) Curacao Gaming Authority AML/CTF/CPF guidelines and regulations, lastly amended in January, 2025

The above-mentioned laws and decrees serve as the basis for the procedures maintained by the Company to detect and deter industry related risks for money laundering, the financing of terrorism, proliferation of weapons of mass destruction or other criminal activities. Money laundering is a criminal offence in Curaçao.

Violation of these laws and regulations are subject to administrative and criminal sanctions

International regulations

As a member of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), which is a Financial Action Task Force (www.fatf-gafi.org) Style Regional Body, Curaçao is meeting International standards by regularly implementing these standards in its national legislation.

On an international level, the FATF plays a very important role in the combating of money laundering, 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 38 countries are direct members of the FATF and through regional organizations over 200 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/CPF. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

6. Role of Compliance

Why is it important to avoid being exposed even innocently to relationships that involve the criminal proceeds?

□ The Company is obliged under the AML/CFT/CPF legislation to comply with the relevant regulations, breach of which can result in large financial losses, license withdrawal, suspension or certain operational restrictions implied by the regulatory authorities or even business loss.

□ Even though criminal liability may not result from relationships about which the Company has no ML/FT/PF knowledge or suspicion, reputational damage that can occur even from innocent handling of criminal property can be very serious and can have devastating impact as on the Company, as much on the employees themselves or even on the country.

□ It is morally and ethically wrong to provide services and products in a way that would facilitate the laundering of criminal property.

Therefore, the Company shall:

- 1) Maintain the Company's good business and integrity reputation;
- 2) Cooperate with the State Supervisory Authorities;
- 3) Regularly conduct employee training sessions to effectively manage AML/CFT/CPF risks;
- 4) Ensure sufficient resources for AML/CFT/CPF compliance and promote their efficient and expedient application at all stages;
- 5) Encourage honest and trustworthy environment in the workplace;
- 6) Eliminate employee doubts or fears that could be linked to filing of suspicious transactions or activity reports;
- 7) Encourage qualitative, as opposed to formal, approach to all AML/CFT/CPF procedures and processes execution.

7. Definition of money laundering

Money laundering is the process by which criminals attempt to hide and disguise the true origin and ownership of the proceeds or any other benefit of their criminal activities, thereby avoiding prosecution, conviction and

confiscation of the criminal funds. Money laundering occurs every time **any transaction** takes place, or any **relationship** is formed that involves **any form of property or benefit** that has **come from any crime**. The **offence** of money laundering occurs whenever **a person or business assists anyone to launder the proceeds of crime** while **knowing or suspecting or having reasonable grounds to suspect** that the property is the proceeds of crime.

Traditionally Money Laundering process is divided into three stages:

- 1) **Placement** – where cash from criminal activity is placed into the financial system/ is converted into monetary instruments
- 2) **Layering** – usually involves a series of transactions designed to hide the source and ownership of the funds and confuse the authorities; and
- 3) **Integration** – where laundered funds are reintroduced into the legitimate economy, appearing to have come from a legitimate source.

The Company does not accept cash as a payment method in any circumstances; therefore, the Company's AML/CFT/CPF Policy places more focus to prevent the use of the Company's activities and resources in the 2nd and in the 3rd stage.

It is important to note, that although the three-stage model of money laundering is a convenient way of describing the activity, it does not always reflect the reality and can be seen as a little simplistic.

How money can be laundered by means of the gaming industry companies?

The money launderers are trying to obscure the origin of the criminal proceeds by channeling them through a gambling platform. The ultimate purpose is to give that money a “clean” look and represent it as the profit / winnings from the gaming activity. There are several scenarios that are popular among the money launderers and the employees need to be vigilant and in case noticed, report such cases to the Compliance Officer in order to prevent such activity on the accounts of the Clients of the Company.

A first scenario is when the client uses various payment methods to deposit funds onto a gaming account. While the linked bank account can be used to do so, many other payment methods can be utilized, such as anonymous credit and debit cards, prepaid cards, cheques and crypto-currencies. After the money was placed on the gambling account the launderer wants to withdraw those funds, thus, giving them a legal status. In this method the Client does not, or to a limited extent only, uses the money for actual gambling.

A second scenario is for the Client to place the money as bets. In this case, the Client will place his money – (e.g., by registering one of the accounts using third party's ID) – in games (e.g., poker, Roulette, Baccarat, Sports betting, etc.) where he can work in close collaboration with other Clients. One Client will deliberately lose, so as to benefit another Client. Even though in this case some costs will occur, it is acknowledged that the criminals are willing to accept such expenses to be able to further benefit from their criminal proceeds. The expenditures they face are not essential compared to the benefits they gain.

A third scenario is that of using the gambling accounts for effecting payment for purchase and sale of illegal goods. In this case both the buyer and the seller of the illegal goods hold a gambling account. Thereby funds can easily be moved from one gambling account to another by way of Client-to-Client transfers. Thus, the seller will receive the money on his gambling account that is further paid out to his payment account appearing to be “clean” and represented again as profit or winnings from the gambling activity, even though it actually is the profit earned by selling goods.

Taking into consideration risks posed by the second and third scenarios the transfers between Clients are prohibited by the Company. Moreover, the Client is not allowed to choose his opponent in any game (the opponent is chosen by the game).

The fourth scenario is when the gambling account is used exclusively for storing money and hiding it from the authorities. The difference with the previous method is that, while in that method the money is paid out as gambling profits, in this method the money is only being concealed and retrieved from the gambling account using the same payment method.

In cases when employees have suspicions that the client is implementing one of the above or similar scenarios, the internal report must be filed to the Compliance Officer. Please refer to the Reporting procedure below for more details on how the report should be filed.

For the list of currently known typologies of suspicious transactions and activities / behaviour of the clients related to gaming industry, please refer to the Annex 1.

The employees should take into consideration that the scenarios along with the list of the typologies of suspicious transactions and activities / behaviour of the clients mentioned above are not exhaustive and new typologies and methods are regularly emerging. The money launderers are constantly developing new methods for their purposes to be implemented. Therefore, the employees must always remain alert and inform the Compliance Officer about any suspicions they have and file the internal reports following the guidelines in the Reporting procedure.

8. What is Terrorism Financing?

Terrorism Financing is the provision of funds or financial support for individual terrorists or terrorist groups or organizations. It is important to note, that terrorism financing comprises not only provision of funds for the commitment of terrorism act, but also includes provision financial support for terrorist cells for their general purposes, e.g. day-to-day operations.

Money laundering and terrorist financing have a number of features in common. Even in cases where the benefit of underlying criminality is being laundered the laundered proceeds will eventually go to fund future or prospective criminal acts. The destination of money used to support terrorism has to be disguised, in the same way that the source of laundered funds must also be disguised. The same methods may be used for both.

Even where the source of funding for terrorist activity is lawful, terrorists will nevertheless attempt to disguise it in order to preserve future funding. A classic example is the collection of charity donations for an organization supporting terrorism. Both money laundering and terrorist financing require the assistance of the financial sector. Terrorist groups have shown a willingness to use emerging technologies, such as prepaid or value stored cards and pre-loaded mobile phones to fund attacks and to provide funds and information to assist the logistics of the attacks.

Terrorist Financing is often seen as money laundering in reverse, because it is often the case that terrorists collect money from perfectly legitimate sources (a charity used as a front for terrorist organizations) – clean money, which is then subsequently used for criminal purposes (e.g. financing the materials for a bomb). Many of the techniques used to disguise the destination of terrorist funds are identical to those used to disguise the source of the proceeds of crime. The difficulty comes in protecting business against property that may have derived from a lawful source but that may be destined to fund future acts of terrorism. Therefore, the employees must be alert to the possibility that property they are handling may, at some future point in time, be used to fund an act of terror or terrorist organization.

9. What is Proliferation of Weapons of Mass Destruction

Proliferation Financing frequently features three elements:

1. Fundraising – funds are raised to finance a WMD programme
2. Disguising – funds are transferred into the international financial system
3. Procurement of materials and technology – funds are used by a proliferator or its agents to pay for goods and services

Possible indicators of PF can be grouped into different categories including the below:

Geographic indicators

- Transaction involves a country of proliferation concern
- Transaction involves country of diversion concern
- Transaction involves a country that presents a proliferation financing risk, or has strategic deficiencies in the fight against ML/FT/PF
- Transaction involves a jurisdiction with weak export control laws or weak enforcement of export control laws
- Transaction involves a financial institution with known deficiencies in AML/CFT/CPF controls or located in a country with weak export control laws or weak enforcement of export control laws

Client /business partner indicators

- The Client or a person or entity in the customer relationship might be engaged in activity which has vulnerability to abuse for proliferation
- Client activity does not match business profile or end-user information does not match end-user's business profile
- The Client or business partner or its address is similar to one of the parties found on publicly available lists of persons designated for proliferation-related reasons
- Client has previously had dealings with individuals or entities that are now designated persons for proliferation and/or proliferation financing reasons
- Client provides vague/incomplete information and is resistant to providing additional information when queried

Transaction indicators

- Delivery of products and/or services that are subject to proliferation-related UN sanctions
- Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose

Differences between Money Laundering, Terrorist Financing and Proliferation Financing

PF differs from ML and TF in the following ways:

- The movement of funds in ML is cyclical, while PF is linear. Funds do not to be returned to the organisation funding proliferation
- PF may not necessarily derive from the proceeds of crime; it may involve the use of legitimately sourced funds
- The focus of ML investigations is usually on the source of funds and whether funds have derived from criminal activity. PF investigations will consider both source of funds and the use of funds for illicit purposes that may have derived from a legitimate source

- FT differs from PF as it is predominantly funded through criminal activity and may involve greater use of informal finance networks or cash couriers in its transactions

10. Client Acceptance Policy

The Company shall not enter into a business relationship with the Client if:

- 1) The Client is younger than 18 years old or as maybe alternatively determined by the Client's citizenship.
- 2) The Client acts on behalf of or represents any third party
- 3) The Client is a legal entity, and not the natural person end user of the services
- 4) The Client is unable to comply with the CDD/EDD requirements;
- 5) It is known that the Client is or has been involved in ML/FT/PF or Sanctions breaches stories
- 6) The Client is resident of a restricted country
- 7) The Client is a Sanctioned Individual
- 8) The client was included in the Company's internal blacklist.
- 9) The Company is not satisfied that the purpose and nature of the business relationship are legitimate, or the risk posed by the Client falls within an unacceptable risk level, which means that the Client would require too many resources to effectively manage the ML/FT/PF risk

All the client categories mentioned above fall into unacceptable risk categories and service for those shall be declined. If at some point of time the Company determines that such a business relationship already exists, the Company shall terminate it and suspend transactions until it can be terminated, subject to instructions from the authorities, where applicable.

There are risk factors, which automatically lead to the Client be assessed as high risk, such as:

- Politically Exposed Persons and their Relatives and Close Associates;
- Clients with links to high risk jurisdictions;
- Clients, whose overall risk is determined to be high based on multiple factors;
- Clients, who use products or payment methods that might favor anonymity; clients, who use new products, which might have heightened ML/TF/PF risks.

For such clients EDD procedure shall be applied as described in detail in Section 19 of this Policy.

As described further in Section 11 Risk Management and Client Risk Assessment, by default all other clients initially are deemed low risk but are constantly monitored to ensure the risk remains low. Otherwise risk categories shall be revised and further CDD or EDD measures based on the new risks determined to be applied as described in detail further in this Policy.

For low risk clients CDD measures as described further in Section 12 are applied. Medium risk clients are also subject to CDD measures, however, based on determined risk factors, some additional measures may be applied. EDD measures are mandatory for all high risk clients. Please refer to Sections 21 and 22 for details on level of ongoing monitoring and periodic review regularity to be applied based on the Client risk category assigned.

The Company has developed the Client Risk Assessment form, which is included as Annex 3 to this Policy and is regularly reviewed and updated. This form contains information on the specific ML/FT/PF risk factors and their level (low/medium/high) to which the Company is exposed to by cooperating with a specific Client.

11. Risk Management and Client Risk Assessment

Client ML/FT/PF risks may be measured by using a number of factors. Application of risk categories can then provide a strategy for managing potential risks by enabling the Company to subject Clients to proportionate controls and oversight. The Company applies a risk-based approach in determining the amount and extension of information and documents that have to be collected from the client. The key risk pillars for the Company are:

- ☐ Country or geographical risk
- ☐ Client risk
- ☐ Product/service /transaction risk
- ☐ Interface / delivery channel risk.

Geographical risk arises from links with one or more geographical areas, usually related to those jurisdictions:

- 1) Where the Client is based, and /or
- 2) With which the Client has relevant personal links (e.g., nationality, residence and place of birth of a Client), and /or
- 3) Where the client has a main place of business or where the activity generating the Client's wealth is carried out.

The Company has developed its Jurisdiction Risk Assessment attached in Annex 7 to this Policy, which lists high risk and prohibited jurisdictions as per the Company's risk assessment. It is regularly reviewed and some jurisdictions may be added or removed from the list, where deemed appropriate.

Client risk is the risk of ML/FT/PF that arises from entertaining business relationship with a given person. This may be due to the business or professional activity carried out by the Client or his source of wealth.

The product, service or transaction risk is the risk the Company is exposed to as a result of providing a given product or service or carrying out a particular transaction. Much will depend on:

- ☐ The level of transparency or opaqueness that the product, service or transaction affords
- ☐ The complexity of the product, service or transaction; and
- ☐ The value or size of the product, service or transaction
- ☐ ability of a customer to influence the outcome of a game

Interface/Delivery channel risk is the risk arising from how the Company interacts with the Client and the channels it uses to provide a given product or service.

Risk classification

The Company classifies Clients into the following ML/FT/PF risk categories:

- ☐ Low risk
- ☐ Medium risk
- ☐ High risk
- ☐ Unacceptable risk.

Initially all the clients are deemed low risk, but their activity is constantly monitored to detect cases, where the risk should be increased. The following risk factors automatically categorize Clients as high risk and so EDD measures described further in this Policy must be applied:

- 1) PEPs, their family members or close associates
- 2) Client's links to high-risk countries
- 3) There is knowledge, suspicion or reasonable grounds to suspect that a client, his activity or the proceeds are related to ML/FT/PF
- 4) Client uses products / payment methods that might favor anonymity
- 5) Client uses new products/services which might pose heightened ML/FT/PF risks

Client Risk Assessment form from the Annex 3 to this procedure must be completed manually and recorded to the Client's Profile by the employees, immediately for the Clients, whose risk is higher than low and for all the Clients, when payments to or from the account are equal or in excess of XCG 4000 or equivalent to that amount in any other currency.

1. The following steps must be taken during Client risk assessment:

- 1) Identification of the risks specific to a certain Client and weighting of each risk according to a scale;
- 2) Manual input of data specific to a Client to the client risk assessment form;
- 3) Verification and evaluation of the Client screening results made via Sumsb to check whether the client has any matches with the individuals from the watchlists (PEPs lists, Sanctions lists / Adverse Media);
- 4) Calculation of total risk score;
- 5) Assigning a risk level according to a total risk score
- 6) Based on the established risk profile of the client, the employee shall proceed with applying CDD or EDD measures described below. The extent of on-going monitoring and periodic assessment measures are also determined based on the risk level of the client as described below.

In the course of business relationship, the Client's risk category may be changed based on the newly identified ML/FT/PF risks.

Client Risk Profile shall be mandatory reviewed in the following cases:

- 1) if inconsistencies with Client's profile or suspicions about fraud occur (including in cases, when multiple payment methods are being used, big deposits detected, frequent deposits or withdrawal requests received by the employees, etc.)
- 2) if there are doubts about the completeness, reliability or accuracy on priorly obtained client information or documentation or the client being evasive or not cooperative to provide the requested information and / or documentation
- 3) during client periodic review
- 4) if Enhanced Due Diligence procedure was initiated

12. Customer Due Diligence

1. The Know Your Client (KYC) process, as part and parcel of the Company's ML/FT/PF risk management, is divided into the following stages:

- 1) Client On-boarding (Registration):
 - Client identification
- 2) CDD / EDD measures in cases as set out further in this procedure

- 3) On-going monitoring
- 4) Periodic assessment

2. Initially, personal details of a potential Client are received through the registration form at the website, where the Client is required to provide the following personal details:

- 1) Full name
- 2) Date of birth
- 3) Permanent Residential Address
- 4) E-mail
- 5) Username and a password;
- 6) Consent to Terms of Use
- 7) Statement that the Player is over 18 years old

3. Screening against sanctions/PEPs, their Family Members and Close Associates/Adverse Media is initiated at this point, including ongoing AML monitoring, which is enabled immediately to control any changes to the status of the Client. Automated screening is performed via Sumsb;

4. If screening results in matches, the Employee shall analyze matches. If true matches are detected, those shall be reported to the Compliance Officer. The Employee shall act in accordance with p.23 of this procedure.

5. The Clients are not allowed to use the services of the Company without registration. The e-mail provided by the Client is verified and only after successful verification the Client can be registered.

6. The Client is added to the Company's secure list of all registered Clients.

7. Upon any payment (or series of cumulative payments) of XCG 4000 or more (or equivalent in any other currency) further CDD procedure must be initiated.

8. During CDD procedure the Employee shall perform the following steps:

- 1) Inform the Client that the Company is requesting information to verify his/her identity.
- 2) Request the ID document, selfie with it and proof of address ;
- 3) Check screening results of the Client against PEPs / Sanctions / Adverse Media lists
- 4) Client risk assessment: The Employee shall complete a Client risk assessment form as set out in Section 11 Risk management and Client Risk Assessment
- 5) Obtaining information on the intended purpose and nature of the business relationship to establish Client's business and risk profile (information should be obtained by asking Clients to complete the KYC Questionnaire from Annex 4 to this Policy)
- 6) The extent and type of additional information to be required from the Client depends on the risk level assigned to the Client. For high risk Clients EDD procedure must be initiated.

9. At this point of time the Client can use his gaming account balance for placing bets, however he is not permitted to make deposits or withdrawals.

10. The Client is prohibited to further deposit or withdraw any funds from his account until the Employee receives all the requested information in terms of CDD/EDD procedure and is satisfied with the quality of the provided information and / or documents.

11. The identification of the Clients shall be conducted on a non-face-to-face basis only.

12. It is prohibited to establish business relationships and/or cooperate with the Clients, who act in the interests of third parties.

13. For the purpose of identity verification all the Clients are asked to provide a scan / photo of:

- 1) Identity Document (list of acceptable ID documents is provided below)
- 2) Selfie made with that ID document (must be made at current time, when the CDD procedure is in progress).
- 3) Address confirmation document (list of acceptable address confirmation documents is provided below)

14. For the purpose of further establishing Client risk profile and nature and purpose of business relationship the Clients are asked to complete the KYC Questionnaire, which shall include the following information:

- 1) Full name
- 2) Date of Birth (only Clients over 18 y.o., or over alternative age as may be determined by the Client's citizenship, are accepted)
- 3) Residential Address
- 4) Occupation / Employment
- 5) Gross annual income
- 6) The expected source and origin of the funds and source of wealth to be used throughout the business relationship
- 7) Information on whether the Client acts on his own behalf and not in the interests/benefit of third parties.
- 8) Information on the PEP status
- 9) Expected gaming patterns, such as the expected deposit amounts monthly

15. The Client is asked to complete the information and/or upload documents on the website that subsequently are reviewed by the Employee in the System or send the documents via authorized registered e-mail and subsequently are uploaded to the System by the Employee.

16. The Employee shall check the expiry date of the identity document, the visual similarity/correspondence of the photo on the identity document with the selfie of the Client,, in cases where EDD measures are applicable check availability of adverse media in public and reliable sources by using search engines, such as Google, LinkedIn, etc.

17. The Employee may use the following public source to make sure the identity document is not fraudulent:

<https://www.consilium.europa.eu/prado/en/search-by-document-country.html>

18. The Employee shall visually check the scanned document for any signs of forgery, damage, etc. Please refer to the link below for additional information on signs of possibly counterfeit documents:

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869551/Guidance_on_examining_identity_documents_v_February_2020.pdf

19. If suspicions about the quality of the identity document occur, the Employee shall immediately contact the Compliance Officer and act further in accordance with his instructions. The Compliance Officer shall review the materials and determine whether further identification is required and/ or whether a report is to be sent to the relevant authorities.

20. If similarity between the selfie and identity document provided is dubious, the Employee may request the Client to provide additional documents.

21. In some cases, the Compliance Officer can instruct the Employee to request an online video identification and interview with the Client, during which the Client will be asked to repeatedly show his/her ID document.

22. After receipt of the information from the Client and if no matches found in the Sanctions / PEP / adverse media lists, the Employee shall conduct Client risk assessment by filling in the Client risk assessment form as specified in Section 11 (Risk Management and Customer Risk Assessment).

23. If during verification possible matches are found, the Employee analyses the hits:

1) If there is a true match with the Sanctioned Individual, the match shall be immediately reported to the Compliance Officer and the business relationship with the Client shall be terminated following the instruction of the Compliance Officer. If the match is a false positive, the Employee shall proceed with the Client risk assessment;

2) If there is a true match with a PEP individual, the match shall be reported to the Compliance Officer along with the Client's details and relevant information obtained, and the Employee shall await further instructions from the Compliance Officer. If the match is a false positive, the Employee shall proceed with the Client risk assessment;

3) If there is adverse information from a reliable source that indicates Client's possible involvement in ML/FT/PF or other illegal activities, the Employee shall report the case to the Compliance Officer by filing internal UTR. The business relationship with the Client shall be suspended and the Employee shall await further instructions from the Compliance Officer. If suspicions are grounded the Compliance Officer files the report to FIU and the person is added to the Company's blacklist. If the match is a false positive, the Employee shall proceed with the Client risk assessment;

27. If the Client is assigned low risk level and the Employee has received all the CDD information and documentation from the Client, and there are no inconsistencies with an average profile of a Client from the same jurisdiction, and the Employee is satisfied with the quality of obtained information and documentation, the Client can proceed to use his account in a usual manner (the payment restrictions are cancelled at this point).

28. If the Client is assigned medium risk level, the volume and type of additional information which may be required would depend on the risk factors specific to the Client. If no specific measures that should be applied immediately are required, the risks should be marked in a client risk assessment form, and if there are no additional ML/FT/PF risk increasing factors, the Client can proceed to use his account in a usual manner (the payment restrictions are cancelled at this point).

29. If the Client is assigned a high risk level, the Employee shall escalate the case to the Compliance Officer by the email. The employee shall provide the Compliance Officer with the Client Profile and await further instructions. The Compliance Officer shall inform the Employee about his decision, whether to terminate business relationship with the Client or to proceed with EDD.

30. If the Client falls within an unacceptable risk category, the Employee shall report the case to the Compliance Officer and the business relationship with the Client should be terminated following the instructions of the Compliance Officer .

31. The Company can continue to cooperate only with those Clients, who have fully complied with all CDD/EDD requirements, the Client's profile is clear to the Company and his risk profile is acceptable in terms of Company's risk appetite.

32. The Employee stores all the documents and information obtained from the Client, as well as completed Client risk assessment form in the Client profile.

33. If the Client does not provide required information / documents within 30 days after reaching the threshold of NAF 4000 or if the Employee is not satisfied that the purpose and nature of the business relationship are legitimate, the Employee shall:

1. Terminate the business relationship with the Client;
2. Consider the need to file an internal unusual transaction report to the Compliance Officer;

Prior to terminating the business relationship with the Client the Employee shall receive the approval from the Compliance Officer

34. ***In case there is a need to file the internal unusual transaction report, the Compliance Officer should be contacted before terminating the business relationship with the Client to ensure the risk of tipping-off offence is mitigated.*** Please refer to the Reporting procedure for the detailed information on how an unusual transaction report should be filed.

35. If the business relationship with the Client is terminated, the Compliance Officer may decide that the Client should be added to the internal blacklist of the Company. In this case, the reason for termination of the business relationship must be recorded.

36. The documents provided by the Client are reviewed and verified by the Employees on the aspects of correctness, inconsistencies with what the Company already knows about the Client.

37. If the Employee receives all the required information from the Client and is satisfied with the quality of the information / documentation, deposit and withdrawal restrictions shall be cancelled.

38. CDD procedure shall be initiated regardless of the amount involved, if there are doubts about the veracity or adequacy of previously obtained customer identification data

39. ***In cases when there is knowledge, suspicion or reasonable grounds to suspect that a Client, his activity or the proceeds are related to ML/FT/PF the EDD procedure must be applied regardless of the amount involved. In such cases the Client shall not be informed about the reason the Company is conducting EDD procedure.***

13.Simplified Due Diligence Rules

The Simplified Due Diligence may be applied only in relation to the low risk clients. Thus, unless there are no risk factors, which might heighten the risk of the Client, including for example risk factors listed in Section 19 Enhanced Due Diligence, the client is deemed to be low risk and the measures described in Section 12 Customer Due Diligence are applied.

In terms of Simplified Due Diligence Rules, at the registration stage the Client provides only the minimum required information, mentioned in Section 12 in detail. This does not apply to higher risk clients, for whom CDD/EDD measures are applied and for whom additional verification may be initiated at the earlier point of time.

For low risk Clients the standard CDD procedure is allowed to be initiated, when reaching the XCG 4000 threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing.

14.CDD and On-Going Monitoring Process Record Keeping

1. The Employee shall record all of the obtained information, as well as the results of procedures conducted in respect of the Client in the Client Profile in the System.
2. The Employee shall verify the obtained information to the extent possible against publicly available reliable sources of information.
3. Documents / information obtained from the independent and reliable sources, including those from internet resources, shall contain the date of verification and name of the source of information and shall be uploaded to the Client Profile.
4. Where applicable, a list of links to public registers can be found in Annex 5 to this Policy. The information about management / ownership of the legal entities in various jurisdictions is available in the said public registers.

15. Correspondence with the Client

1. The Client shall submit the information via the personal account on a website or an authorized e-mail address. The information / documents subsequently are displayed in the System.
2. The Employee is allowed to accept information / documentation from the Client submitted through the website or an authorized e-mail address only.

16. Document Translation and Certification

Where there is a doubt as to the integrity and the reliability of the document, the independence of the entity issuing the documents or, considering specific risk profile of a given transaction or Client, the Employee may require certification of documentation.

The document can be deemed properly certified, if:

- 1) A public document or the copy of a document has been first certified by a notary public or a public officer with equal rights (for instance the representative of the state register). For EU, EEA member states and Swiss Confederation certification by a notary public or an equal officer is sufficient.
- 2) An apostille is required for documents issued in countries that have joined the Hague Convention Abolishing the Requirement of Legalisation for Foreign Documents as of 5 October 1961.
- 3) Legalization is required for documents issued in countries that have not joined the Hague Convention Abolishing the Requirement of Legalisation for Foreign Documents of 5 October 1961.

The documents should be in English or in a language which is understandable for employees and which can be easily translated into English, when necessary. Document translation must be certified as a true translation of the original.

17. Acceptable Identity Verification Documents

The expiration date of the documents at the moment of initial CDD procedure shall not be less than 1 month:

- 1) Passport;
- 2) National Identity Card
- 3) Driver's license
- 4) Residence Permit

Other types of documents based on the issuing country shall be subject to approval by the Compliance Officer.

18. Acceptable address confirmation documents

The documents confirming Client's address should be ***not more than six months old*** at the moment, when the CDD procedure is being conducted.

- ☐ A recent statement or reference letter issued by anyone carrying out relevant financial business or equivalent activities in a reputable jurisdiction;
- ☐ A recent utility bill for a service installed and provided at a residential property;
- ☐ Correspondence from a central or local government authority, department or agency;
- ☐ A lease agreement (*it need not have been entered into in the six months preceding the CDD procedure, but the lease must still be current at the time of procedure*);
- ☐ An official conduct certificate;
- ☐ Any other government-issued document not mentioned above; or
- ☐ The mailing of correspondence via registered mail or by means of a courier which allows the Company to obtain documentary evidence that the correspondence was effectively delivered at the residential address provided by the Client and signed for by the same.

Other acceptable documents shall be subject to approval by the Compliance Officer.

19. Enhanced Due Diligence

1. The Company must apply EDD measures in those situations that, by their nature, represent a higher risk of ML/FT/PF. In essence, EDD measures are additional measures to the CDD measures set out above, which are to be applied to ensure that the higher risks presented by certain Clients are better monitored and efficiently managed to avoid any involvement in ML/FT/PF.
2. If the case occurs, where EDD must be conducted, the Employee shall inform the Compliance Officer accordingly by e-mail and submit the Client Profile. The Compliance Officer shall acknowledge the receipt of the e-mail and instruct the Employee on the decision made: whether the business relationship with the Client shall be terminated or whether further EDD measures should be applied.
3. The extent of additional information sought, and of any additional monitoring measures carried out in respect of a particular Client will depend on the specific ML/FT/PF risks that the Client was assessed to present to the Company.
4. The cooperation with the high-risk Client, for whom EDD measures shall be applied, shall be approved by the senior AML officer.
5. The following cases are obligatory for the Company to conduct EDD procedure:

- ☐ Residents of high risk countries
- ☐ The Client has been assigned a high-risk category, including PEPs and their family members or close associates;
- ☐ In case of fraud suspicions
- ☐ There is publicly available information about the Client's connection with ML/FT/PF;
- ☐ The Client uses products/services/payment methods that favor anonymity
- ☐ The Client uses new products or services which might pose heightened ML/FT/PF risks

6. Examples of Enhanced Due Diligence measures that can be applied:

- ☐ Requesting additional identification documents;
- ☐ Requesting video identification of the Client, where the Client can be additionally asked about his personal or business activities, confirming the information previously obtained from the Client;
- ☐ Requesting selfies with all the documents submitted by the Client;
- ☐ Requesting notarized or similarly duly certified copies of documents;
- ☐ Requesting additional documents relevant to the Client's employment / business/ previous address;
- ☐ Requesting additional documents confirming source of funds for a particular transaction;
- ☐ Requesting additional documents confirming Client's source of wealth;
- ☐ Requesting additional information about the intended purpose and nature;
- ☐ Requesting senior management approval;
- ☐ Conducting enhanced monitoring of the business relationship
- ☐ Other measures as may be indicated by the Compliance Officer;

In situations presenting a higher risk of ML/FT, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the Client.

20.EDD during the course of business relationship

Other events that can trigger EDD:

- 1) The Client has been assigned high risk level after his risk profile re-assessment;
- 2) The Client became a PEP;
- 3) Unusual transactions;
- 4) Unusual betting patterns;
- 5) Change of gaming patterns (e.g. sudden opting for a higher risk products)

- 6) Publicly available information about the Client's connection with ML/FT/PF and Sanctions, any other illegal activity, Sanctions breaches, their circumvention or an attempt thereof
- 7) The Employee becomes suspicious that the transactions performed by the Client are connected with ML/FT/PF, any other illegal activity, Sanctions breaches, their circumvention or an attempt thereof;
- 8) A request from the FIU, other supervisory authorities or court has been received regarding Client's possible involvement in ML/FT/PF and Sanctions or other crimes;
- 9) Other factors that could pose the Company to higher ML/FT/PF risk exposure.

The Employee shall record the EDD measures applied and the results of the process in the Client profile.

When EDD measures are applied during the course of business relationship the Client risk profile has to be reviewed and information in the Client Risk assessment form has to be updated accordingly.

The records of EDD process should be saved in a specifically created word-file and contain the following information:

- 1) The date on which EDD procedure was initiated;
- 2) The period of EDD;
- 3) If applicable, quantitative limits or other restrictions applied to the account of the Client;
- 4) Requests of additional information, documents and clarifications from the Client;
- 5) Additional measures, determined as a result of EDD and which should be further applied to the Client (e.g., enhanced transaction / activity monitoring, more frequent periodic assessment, etc.)
- 6) The name of the Employee who performed EDD.

The following factors should be taken into account when analysing the Client Profile:

- ☐ Information on the Client already held by the Company;
- ☐ Information which can be obtained through public sources, such as the internet;
- ☐ Nature and purpose of the business relationship;
- ☐ Payment methods used by the Client;
- ☐ Games played;
- ☐ The Client's playing trends and patterns;
- ☐ Betting patterns;
- ☐ Gaming activity turnover (ratio against deposits)
- ☐ Deposits followed by quick withdrawal requests;
- ☐ Patterns of possible structured transactions;
- ☐ Patterns of seemingly linked transactions;
- ☐ Information about source of funds or source of wealth;
- ☐ Results of screening against PEPs / Sanctions / Adverse media lists;
- ☐ Pattern of previously considered unusual and/or suspicious transactions;

- Other relevant information.

The results of possible detected deviations and made conclusions should be reported to the Compliance Officer via the e-mail. The risk category of the Client should be indicated in the report. The Compliance Officer shall decide whether to continue business relationship with the Client with / without future restrictions or to terminate the business relationship and shall instruct the Employee accordingly. If during the EDD procedure the Employee detects suspicious transactions/activity, the Employee shall file an internal UTR and act as set out in the Reporting procedure.

In situations presenting a higher risk of ML/FT/PF, source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the Client.

21. On-going monitoring

It is the obligation of the Company to ensure the on-going monitoring of the business relationship with their clients. On-going monitoring consists of the following segments:

- 1) Ensuring that the documents, data or information held on the Client are up to date.

For this purpose the Employee obtains fresh identification documents from the active Clients, when the expiry date of previously obtained documents is reached. Upon receipt, the document shall be reviewed and checked as described above in Section 12 Customer Due Diligence and saved to the Client Profile.

- 2) Scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the Company's knowledge about the Client and its risk profile;

The essentials of any monitoring process are:

- 1) The detection of possible ML/FT/PF instances for further examination;
- 2) Appropriate measures applied based on the findings.

The activity of all the Clients, regardless of the risk, is constantly monitored. Where the Company notices that the Client's account activity is not in keeping with what it knows or expects from the Client (e.g., activity not justified on the basis of the Client's source of wealth or not in keeping with the average profile or account activity noted to date, activity does not reflect the Client's usual transactional patterns etc.), the Company has to question this unusual activity and, where necessary, establish the source of the funds used for the said activity.

The scrutiny of the Client's transactions is implemented in the following way:

The pattern of Client's transactions is always analysed by the Employees for the aspects of possible ML/FT/PF and other types of fraud during each CDD/EDD procedure or when automated System report has been received or in any case before any withdrawal of funds can be processed.

The following aspects are taken into consideration:

- nature and purpose of the business relationship;
- payment methods used by the Client and frequent change of payment methods
- games played;

- ☐ the Client's playing trends and patterns;
- ☐ betting patterns and amounts spent versus deposits made
- ☐ any information on the Client already held by the Company
- ☐ information which can be obtained through public sources, such as the internet
- ☐ patterns of possible structured transactions
- ☐ patterns of seemingly linked transactions
- ☐ frequent deposits and withdrawals
- ☐ information about source of funds or source of wealth
- ☐ results of screening against PEPs / Sanctions / adverse media lists
- ☐ Pattern of previously considered unusual and/or suspicious transactions;
- ☐ Frequent IP address changes / account being used from several IP addresses at the same time / IP address country is different from the declared residential country / same IP for different users
- ☐ Potential indicators of Client having multiple accounts
- ☐ Attempts to use a third party payment methods, changes in personal data, behavior and activity changes as well as checks, if an account is used by its original owner
- ☐ Other relevant information.

In addition the following automated tools are used for transaction monitoring:

- ☐ The System red flags the Clients, who request withdrawal without sufficient gaming activity
- ☐ The System generates the reports of players who make frequent deposits and withdrawals/large deposits or withdrawals
 - ☐ The System generates the reports of players who reach certain verification thresholds
 - ☐ The System generates daily reports of players whose transactions are equal or above 4000 XCG along with all the details of the users making those transactions.

Above-mentioned alerts shall be reviewed by the Employee and the Employee shall determine whether there are any inconsistencies with the Client's profile, whether additional information, explanation or documentation shall be requested from the Client. If a transaction appears to be suspicious or cannot be rationally explained, the Employee escalates the case to the Compliance Officer and acts upon his/her further instructions.

The withdrawals are temporarily blocked for these Clients until the moment when alert is cleared.

To the extent the Company utilizes a third party to process and record payments to and from Client and accounts, the Company will use best efforts to ensure the service providers 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 Compliance Officer shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

22. Periodic review

As part of on-going monitoring process, the Company must also question the data and information already in the Company's possession whenever any inconsistencies with the same arise, however noticed.

1. The periodic review of the Company's Clients shall be performed to all the Clients, for whom obligatory CDD measures have been applied.
2. The periodic review is required to ensure that the Company's knowledge of a particular Client and risk profile assigned to it is in line with the Client's actual activities.
3. Periodic review is conducted immediately upon material change. If this is not the case then on a risk sensitive basis. Depending on the assigned risk level, the date on which periodic review shall be scheduled, should be determined as described below:
 - ☐ High risk Clients shall be reviewed every 12 months
 - ☐ Medium risk Clients shall be reviewed every 18 months
 - ☐ Low risk Clients shall be reviewed every 3 years
4. The accounts of the Clients, whose risk category after risk profile re-assessment was defined as unacceptable, shall be closed following the approval of the Compliance Officer.
5. The purpose of the Periodic review is to update information about the Client, ensure that the Company's knowledge about its Clients remains actual and valid, the identified ML/FT/PF and Sanctions risk increasing factors and the determined risk level have not changed, that the transactions conducted by the Client are consistent with previously declared ones and do not pose suspicions about ML/FT/PF, there is no adverse information in publicly available sources of information, any other illegal activity, Sanctions breaches, their circumvention or an attempt thereof, ensure that the Company has at its disposal current information on the Client and its activities, supporting documents, and update the Client's risk profile by filling in the client risk assessment form based on the results of the periodic review.
6. In terms of the periodic review the Client will be required to complete a new KYC Questionnaire to determine whether there are any changes to his profile.
7. If during the periodic review the Employee detects suspicious activity, the Employee shall act in accordance with the Reporting Procedure.
8. For High risk Clients EDD measures should be applied during periodic assessment and results approved with the senior AML Officer. For such Clients periodic assessment is deemed to be completed, when EDD procedure has been completed and relevant records have been made as described below.
9. Periodic review is deemed to be completed, when the Employee receives the new KYC Questionnaire from the Client, evaluates any changes to the Client's profile, updates Client risk assessment form and records the results of periodic assessment as set out below.
10. Results of the Periodic review shall be recorded in a specifically created word-file and saved in the Client Profile.
11. The records of Periodic review shall contain the following information:

- The date on which the periodic review took place;
- Whether risk level assigned to the Client has changed;
- Any additional findings / updated information about the Client;
- Full name of the Employee, who performed the periodic review.

12. The date for the next periodic review has to be set by the Employee in accordance with the new (or unaltered) risk level assigned to the Client, on the day, when periodic assessment has been completed.

23. Crypto Usage Policy

The Company is committed to ensuring safe, secure, and compliant operations concerning cryptocurrency payments within its online gambling services. The Crypto Usage Policy defines the approach the Company employs in handling cryptocurrency-related risks, particularly in the areas of verification, transaction monitoring, AML compliance, data security, and fraud prevention. This policy applies to all cryptocurrency transactions processed by the Company and extends to all personnel involved in the handling, monitoring, and processing of these transactions.

The Company considers usage of cryptocurrency as a payment method posing higher risk than traditional payment methods and implements a more stringent customer verification process to ensure that all users engaging in cryptocurrency transactions are accurately identified.

Additional measures to be applied in respect of the clients, who use cryptocurrency as a payment method:

- 1) The threshold triggering CDD procedure shall be XCG 500 of total deposits/withdrawals.
- 2) Any withdrawals shall be made to the same wallet, which has been used for placing deposits, otherwise the control over the wallet shall be established in terms of the CDD procedure
- 3) Enhanced transaction monitoring, as described in more detail below shall be applied and an additional list of indicators of suspicious activity relating to the use of cryptocurrency must be considered. The list is included in Annex 1 to this AML/CFT/CPF Policy. When dealing with the Client who uses cryptocurrency as a payment method, besides being vigilant to the traits of suspicious activities related to fiat currencies, the employees must also consider indicators specific to the use of cryptocurrencies.
- 4) Red flag indicators should always be considered in context. The mere presence of a red flag indicator is not necessarily a basis for a suspicion of ML, FT or PF, but could prompt further monitoring and examination. Ultimately, a Client may be able to provide an explanation to justify the red flag indicator, business or economic purposes of a transaction.

The Compliance Officer shall ensure that verification measures are consistently applied and adjusted as necessary to account for the evolving nature of cryptocurrency risk. The policy shall be periodically reviewed to maintain alignment with regulatory standards and industry best practices. The CO shall oversee the continuous improvement of fraud prevention measures, considering the dynamic risks associated with cryptocurrency and adapting controls as necessary

Transaction Monitoring

The Company uses monitoring systems to review cryptocurrency transactions, ensuring the detection of anomalies or patterns associated with potential money laundering or fraudulent activity.

Each transaction undergoes screening based on transaction limits, frequency, and known cryptocurrency red flags, including rapid, high-value deposits and withdrawals, and usage of anonymity-enhanced cryptocurrency

(AEC)¹, such as Monero (XMR), Zcash (ZEC), Dash (formerly Darkcoin) and other comparable assets or mixing services .

Automated alerts are generated for suspicious activity, which is escalated to the Compliance Officer for further review and potential reporting to the Financial Intelligence Unit Curaçao (FIU).

The escalation of the suspicious activity shall be conducted in accordance with the Internal and External Reporting Procedures.

Anti-Fraud Measures

The company implements fraud detection systems to identify and prevent fraudulent activity associated with cryptocurrency transactions. This includes IP tracking, device monitoring, and behavior analytics.

Manual reviews are conducted on flagged transactions, and suspicious accounts are promptly frozen pending investigation. The Company shall close accounts in cases where fraud is confirmed, with all actions documented in compliance with regulatory reporting requirements.

All relevant staff receive mandatory training on the specific risks, controls, and procedures associated with cryptocurrency transactions. Training sessions cover the identification of red flags, proper transaction monitoring protocols and AML procedures tailored to cryptocurrency usage.

24. Politically Exposed Persons

1. The Company shall determine, whether the Client is a PEP (regardless whether he is foreign or domestic), a family member or a known close associate of a PEP.
2. PEPs are the individuals (together with immediate family members and known close associates), who are or have been, within the last 12-18 months²³, entrusted with a prominent public function in Curacao or outside it. PEPs include, but are not limited to:
 - ☐ 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 any judicial body 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, charges d'affaires and high-ranking officers in the armed forces;
 - ☐ Members of the administrative, management or supervisory bodies of state-owned enterprises;
 - ☐ Anyone exercising a function equivalent to those set out above within an institution of the European Union or any other international body.

Family member of a politically exposed person includes:

¹ <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf.coredownload.pdf>

²FATF Recommendation 12-22 on PEPs

<https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf.coredownload.pdf>

³

https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2017_no_92_landsverordening_identificatie_bij_dienstverlening_gt.pdf

- 1)The spouse, or any person considered to be the equivalent to a spouse;
- 2)The children and their spouses, or persons considered to be the equivalent to a spouse; and
- 3)The parents;

Close associate of a PEP means a natural person known to have:

- 1)Joint beneficial ownership of a body corporate or any other form of legal arrangement or any other close business relations with that PEP;
 - 2)Sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.
3. At the on-boarding stage all the customers are asked to provide information in a self-declaration form by completing registration data needed to identify the Customer. As mentioned above, the Clients are asked to provide their full name, date of birth, permanent residential address, e-mail and account credentials. The sanctions/PEPs/Adverse Media screening via Sumsb is performed at this point to determine the status of the Client.
 4. Where potential matches are detected, the Company also uses publicly available reliable information to determine and / or verify the PEP status of a customer. The status verification is being conducted before commencement of the business relationship with a customer. The status is also constantly monitored during business relationship with the client by using AML ongoing monitoring tools provided by Sumsb.
 5. In cases, when the client is a PEP / a Family member of a PEP / a known close associate of a PEP and his status is established before commencement of the business relationship, the Employee shall report the case to the Compliance Officer and the business relationship with the client shall be declined.
 6. If a true match with a PEP status is established during business relationship with the customer, the match shall be reported to the Compliance Officer along with the customer's details and relevant information obtained, and the Employee shall await further instructions from the Compliance Officer. The Compliance Officer shall decide whether to terminate business relationship with the customer or to proceed with enhanced due diligence.
 7. In terms of Enhanced Due Diligence the following measures shall be applied to a PEP:
 - 1) The Client shall be assigned a high-risk level;
 - 2) Documents, confirming source of funds and source of wealth must be obtained from the customer and further EDD measures as may be suggested by the Compliance Officer shall be applied;
 - 3) Increased transaction monitoring shall be applied;
 - 4) The business relationship with such a customer is subject to the approval by the Compliance Officer.

25.Sanctions

Sanctions are **restrictions** used by international communities as part of an attempt to stop financial crime and terrorism. They are designed as attempts to change the behavior of a targeted country, regime or individuals

where diplomatic efforts have failed. Sanctions can take the form of **economic, trade, financial services or international movement** (travel bans) prohibitions.

The main international sanctions bodies

UN Sanctions

The United Nations Security Council publishes the names of individuals and organisations subject to UN financial sanctions in relation to involvement with ISIL (Da'esh), I-Qaeda, and the Taliban. All UN member states are required under international law to freeze the funds and economic resources of any legal person(s) named in this list and to report any suspected name matches to the relevant authorities. The UN has in place other sanction lists pertaining to other jurisdictions, entities and individuals, including wider terrorist activity under UNSR 1373.

The UN consolidated sanctions list is available at the following link:

<https://www.un.org/securitycouncil/content/un-sc-consolidated-list>

EU Sanctions

The European Union applies sanctions or restrictive measures in pursuit of the specific Common Foreign and Security Policy (CFSP) objectives set out in the Treaty of the European Union. Restrictive measures imposed may incorporate UN Security Council sanctions or EU autonomous sanctions. The latter cannot be imposed against individuals or entities where there is no foreign policy dimension.

Link to the EU sanctions regimes: <https://www.sanctionsmap.eu/#/main>

OFAC Sanctions

The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers and enforces economic and trade sanctions based on the US foreign policy and national security goals against targeted foreign countries and regimes; terrorists; international narcotics traffickers; and those engaged in activities related to the proliferation of weapons of mass destruction; and other threats to national security, foreign policy or the economy of the US. It is important to note that while US sanctions do not directly apply to non-US companies outside the US, the use of the US dollar currency automatically engages OFAC regulations. US prosecutors take the view that if a financial transaction has cleared in the US (as do all US dollar payments, in New York), the US has jurisdiction over the offence. OFAC publishes a list of 'specially designated nationals' or SDNs (known as the SDN List) whose assets are blocked and firms, including US persons, are generally prohibited from doing business with them.

The OFAC Sanctions List Search is available at the following link:

<https://sanctionssearch.ofac.treas.gov/>

UK Sanctions

HM Treasury is responsible for the implementation and administration of international financial sanctions in the UK; domestic designation; licensing exemptions to financial sanctions; and maintaining lists of parties subject to sanctions

The UK Sanctions List Search is available at the following link:

<https://sanctionssearchapp.ofsi.hmtreasury.gov.uk/>

All the potential customers of the Company are screened against current Sanctions lists prior to commencement of business relationship via Sumsb. The screening is also performed during business relationship by using Sumsb AML ongoing monitoring tool which allows the Company to be informed of the potential changes to the status of the Client immediately.

26. Dealing with sanctioned persons

In case when employee during Client on-boarding, CDD or EDD procedure, or during Client ongoing monitoring becomes in the possession of the information that the Client is a sanctioned individual or has any links to sanctioned individuals and / or entities, he MUST:

- ☐ Immediately freeze all the funds / economic resources of the Client available to the Company;
- ☐ Not enter into any financial transactions or provide financial assistance or services to the Client;
- ☐ Apply Enhanced Due Diligence measures;
- ☐ Immediately inform and file the internal unusual transaction report to the Compliance Officer;
- ☐ Suspend the account of the Client until further instructions from the Compliance Officer.

It is prohibited to inform the Client or any third party (except a senior manager or Compliance Officer) in advance, that a measure is to be applied.

The Compliance Officer has to review the internal report as soon as practicable and, in case there are reasonable grounds to suspect that the Client is the sanctioned individual from the lists provided by OFAC, EU or UN, UK the Compliance Officer shall file the external report to the Curacao FIU via the online reporting portal at the following link: https://portal.fiucuracao.cw/goAMLWeb_PRD/Home

Failure to comply with the freezing and reporting obligations can result in the imposition of corporate and personal fines.

Moreover, the Company shall terminate the business relationship with the Client, if there is reliable information about Client's involvement in Sanctions breaches.

27. Termination of the business relationship

1. If a potential or existing Client either refuses to provide the information described in previous sections when requested, or appears to have intentionally provided misleading information and / or the Company is not satisfied with the volume and / or quality of the provided documents the Company will not open a new account and consider closing any existing account. In either case, the Compliance Officer will be notified so that it may be determined whether a report should be sent to the relevant authorities.

2. In any case, the Client's account shall be blocked if the client has not provided requested documents within 30 days after reaching the transaction threshold of total deposits and withdrawals of XCG 4000.

3. It should be noted, that the reluctance of the Client to provide CDD documentation on its own should not be automatically equated to a suspicion of ML/FT/PF. However, the risk of ML/TF/PF should be

considered before terminating the business relationship, taking into account all factors and information the Company has at its disposal about the Client.

4. Thus, where it was decided to close the account of a Client, the Employee shall:

- 1) Consider, if there is a potential ML/FT/PF risk, which could be a reason for Client's reluctance to provide required information. To assess this risk, all factors should be considered, such as payment method used, the games played and the Client's playing trends and patterns, any information on the Client that the Company already is in possession of, including jurisdiction of Client's residence, and publicly available information.
- 2) Save the attempts of relevant document / information inquiries from the Client in the e-mail;
- 3) Block the account as set out below after approval with the Compliance Officer.

If the Client provides the required information and / or documentation to the Company after account suspension, the Employee shall consider whether the delay in providing the CDD documentation and/or information can give grounds to ML/FT/PF suspicions.

If there are no grounds to suspect ML/FT/PF and there are no other rejections from the Compliance Officer, the Client's account can be reinstated.

If there are grounds to suspect ML/FT/PF, the internal unusual transaction report has to be filed to the Compliance Officer in accordance with the Reporting Procedure.

If the account is closed and there are Client's funds available on the account and there are no ML/FT/PF suspicions related to the Client of his funds, the following steps should be taken:

- 1) Consider whether there is any other legal impediment to the remittance of the funds;
- 2) Where applicable, all the winnings shall be void
- 3) Remit the remaining funds to the same source through the same channels used to receive the funds.
- 4) In the event it is impossible to remit the funds to the same source through the same channels, the Employee shall formally request for details of another payment method that must be confirmed to be in the Client's name and hence minimising the risk of remitting funds to an individual other than that who originally made the deposits.
- 5) In the event that these instructions give rise to a suspicion, the Employee should submit an internal UTR to the Compliance Officer and suspend the remittance pending the instructions of the Compliance Officer.
- 6) Whenever the funds are remitted to the Client in the circumstances described above, the indication that the funds are being remitted due to inability to complete CDD should be remarked on the remittance purpose, where possible.

Also, The Company shall terminate its business relationship with the Client in the following cases:

- 1) The Company is in possession of the reliable information about Client's involvement in ML/FT/PF, Sanctions breaches.
- 2) The Client has been assigned unacceptably high ML/FT/PF and Sanctions risk;
- 3) UTR has been filed in relation to the Client;
- 4) The Client is a sanctioned person;
- 5) There are reasonable grounds to suspect that the funds of the Client may be related to ML/FT/PF
- 6) The Client has been identified as attempting or participating in any criminal or unlawful activity

28.Compliance Officer

Currently appointed CO : Maksims Rutenberg

Contact details:

e-mail: rutenbergmaksims@gmail.com

Responsibilities of the Compliance Officer

The Compliance Officer core functions are:

1. To review internally received reports from the Company's employees, or through software solutions used for completeness and accuracy; to further consider these reports, conduct further investigations if needed, determine whether knowledge or suspicion of ML/FT/PF subsists and to decide whether the report should be filed to FIU subject to reporting under the Ministerial Decree on Indicators for Unusual Transactions.
2. Where such knowledge or suspicion subsists, the Compliance Officer must file the UTR to FIU via https://portal.fiucuracao.cw/goAMLWeb_PRD/Hom
3. To analyze transactions, on information or matters that may give rise to knowledge or suspicion of ML/FT/PF, or that a person may have been, is or may be connected with ML/FT/PF;
4. To respond promptly to any request for information made by the FIU.

Other responsibilities of the Compliance Officer:

- ☐ Monitoring of the day-to-day application of the measures, policies, controls and procedures adopted by the Company to ensure continued compliance with its AML/CFT and Sanctions Regimes obligations.
- ☐ Ensuring compliance with Curaçao laws and regulations regarding money laundering and terrorist financing
- ☐ Development and implement AML program, incl. necessary AML/CFT/CPF, Sanctions Compliance policies, controls and procedures and maintaining those up-to-date and in line with any advice and/or guidance from the CGA, Financial Intelligence Unit, and/or other relevant authorities;
- ☐ Design an internal procedure about when reporting of unusual transactions will lead to blocking/ freezing of user accounts
- ☐ Addressing any regulatory feedback about the Company's risk management performance or AML/CFT measures, policies, controls and procedures;
- ☐ Ensuring regular training and education to the staff of the Company in respect of AML /CFT/ CPF policies, controls and procedures, as well as relevant up-to-date legislative requirements and other compliance related matters
- ☐ Reporting to the board on a regular basis to highlight any changes in the AML/CFT/CPF and Sanctions Regimes Compliance framework, Company's efforts against money laundering, terrorism financing, and proliferation financing
- ☐ Regular oversight reporting, including reporting of non-compliance, to the Board;
- ☐ Maintaining a record of decision making as part of the reporting procedure
- ☐ Maintaining a register of disclosures and register of ML/FT enquiries;

- register, compile, handle, as well as provide the information to the relevant authorities about all the suspicious transaction / activity reports.
- filing the internal and external reports to the specially designated registers as soon as practicable and make it available to the relevant authorities upon their request
- Ensuring records are retained in an appropriate format and for the relevant time period in accordance with the Company's AML/CFT/CPF Policy.
- Staying informed about local and international developments related to money laundering and terrorist financing and suggesting improvements to management

The Compliance Officer is not allowed to disclose any information about the filed report, including the information that the report was filed, to the client or to any other third unauthorized person. Taking into account the constantly emerging new typologies and indicators of possible money laundering and terrorist financing, the Compliance Officer also provides the relevant authorities with the information about newly discovered ML/FT/PF typologies and indicators.

29. Reporting Requirements

As already mentioned above, money laundering occurs every time **any transaction** takes place or any **relationship** is formed that involves **any form of property or benefit** that has **come from any crime**. **The offence** of money laundering occurs whenever **a person or business assists anyone to launder the proceeds of crime** while **knowing or suspecting or having reasonable grounds to suspect** that the property is the proceeds of crime.

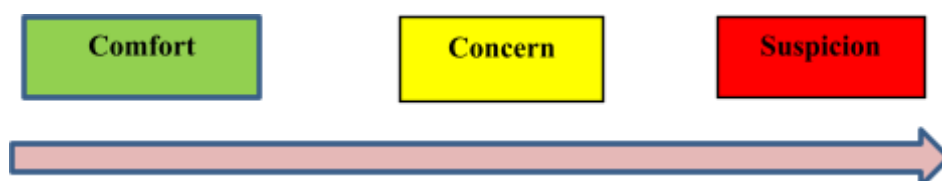
What constitutes knowledge?

There are several types of knowledge including:

- actual subjective knowledge – you definitely know some fact(s), e.g., you know the money comes from drug deals
- willfully shutting your eyes to the obvious (Willful Blindness). This is where you don't ask questions because you think they may raise information that will mean you have to make a report; here you could be seen as having 'known' but turned a 'blind eye' – for example you think the money comes from a crime but you don't make any further enquiries.

What is suspicion?

Suspicion falls short of proof based on firm evidence but it seems clear that there must be a factual basis upon which it can be founded. The formulation of a suspicion is generally a gradual process, it rarely happens instantly. The formulation of suspicions generally follows the following pattern:



An event will happen within a normal client relationship which triggers a concern in the mind of an employee. Once concerned the employee should:

1. Analyze the available CDD and information
2. Discuss concerns with superior manager or Compliance Officer
3. Make discreet enquiries of clients – although client enquiries must be handled carefully in case of suspicions to avoid the offence of tipping off as described below in Section 33 “Tipping Off”. Following this process there will either be a return to feeling comfortable with the client if concerns are allayed, or concerns will remain or shift to being suspicions. If the employee remains concerned then further enquiries should be made or the matter should be referred to a superior manager or Compliance Officer.

Reasonable grounds to suspect

Where a person should have had a suspicion, taking into account all the relevant information.

In the event that the employee formulates knowledge or suspicion either that a client is engaged in criminal conduct or that the property that forms part of the relationship has derived from crime, the employee must make a report. These are known as unusual transaction reports (UTRs) or suspicious activity reports (SARs). The duty to report suspicious activity, including possible terrorist financing activity, rests with every employee within the Company. **There is no requirement for the employee to suspect a particular type of criminal conduct.** It is enough for the employee to simply suspect ‘criminality’ in the broadest sense. Very often it is a combination of factors or features within a relationship that will lead to a suspicion about the relationship as a whole.

Identifying money laundering and terrorist financing activity is a challenge and the employees of the Company should never assume that it is not an issue, even with existing Clients that the company has dealt with for some time (including any VIP Clients). The existing Client relationships pose as great money laundering or terrorist financing threat as new Client relationships, if not a greater one as the Company can become complacent about them. The employees are not expected to play the role of detectives or actively search for information that may lead to suspicion. Instead, during the normal course of the day-to-day activities, the aim is to:

1. **Gain knowledge** of the Clients;
2. **Remain alert** to the possibilities of money laundering terrorist financing, proliferations of WMD;
3. **Consider** whether any Client’s activity is unusual and potentially suspicious (see Annex 1 with the list of potential indicators of ML/TF/PF)

Where an employee identifies any **suspicious** activity in the course of an on-going Client relationship, the employee must –

- (a) conduct enhanced Client due diligence, unless the Employee reasonably believes conducting EDD will tip-off the Client;
- (b) make an internal disclosure (internal UTR).

Where an employee identifies any **unusual** activity in the course of an on-going Client relationship, the employee must –

- (a) perform appropriate scrutiny of the activity;
- (b) obtain enhanced Client due diligence; and
- (c) consider whether to make an internal disclosure (internal UTR).

All internal UTRs should be made in writing as this provides the employee with statutory protection, particularly if the Compliance Officer subsequently decides not to report the suspicion to the authorities.

30. Reporting Procedure: Internal reporting

If the employee knows, suspects or has reasonable grounds to suspect that funds, ***regardless of the amount involved***, are the proceeds of criminal activity or are related to funding of terrorism/proliferation of WMD, or that a client may have been, is or may be connected with money laundering or the funding of terrorism, or that an attempt has been made to carry out a transaction or activity related to such proceeds or funding of terrorism, **the employee must file the internal unusual transaction report to the Compliance Officer.**

In case, when the employee notices one of the indicators of suspicious activity or suspicious transaction listed in Annex 1 to this Policy (“Indicators of Suspicious Activities”), or the employee has suspicions of ML/FT/PF in respect of the client but there is no suitable indicator in the list provided, the employee **MUST** consider making the internal unusual activity report to the Compliance Officer and send it to the e-mail rutenbergsmaksims@gmail.com as soon as possible within the same day when suspicion has been formed, following the steps described below:

1. Send an e-mail from your work e-mail to rutenbergsmaksims@gmail.com with the e-mail subject “Internal UTR Submission”.
2. Complete the form named “Internal Unusual Transaction Report to the CO” from Annex 6 and attach it to the e-mail
3. In the above-mentioned form set out the client ID, the transaction(s) or activity relating to what makes you suspicious. Set out a brief explanation as to why you are suspicious that the transaction or activity may relate to money laundering or terrorist activity and indicate the status of the account (e.g., the account has been suspended) and specify whether any other action (if any) has been undertaken (e.g., the assets have been frozen).
4. To the e-mail attach all relevant documents and information related to the client and to the transaction in question.
5. The CO will acknowledge receipt of the Employee’s e-mail in writing, review the case and advise on any next steps
6. Where the employee knows or suspects that a transaction is or may be related to proceeds of criminal activity or the funding of terrorism, the Employee shall not carry out that transaction until further instructions from CO .
7. Where refraining from carrying out any such transaction is likely to frustrate efforts of investigation or pursuing the beneficiaries of the suspected money laundering or funding of terrorism operations, the Compliance Officer shall accordingly inform the Financial Intelligence Unit immediately after the transaction is affected.
8. If the suspicion relates to a third party, the employee shall set out the details of the third party and what information has made the employee suspicious about them.
9. When the CO receives an internal unusual transaction report, he reviews it immediately, but not later than the next working day. The CO shall consider all the provided and other available information and shall decide whether the external unusual transaction report should be filed to FIU or not.
10. Where, following the consideration of an internal report the CO determines that no reporting to the Financial Intelligence Unit is required, the CO shall record the reasons for such determination in writing to the register of Internal Unusual Transaction Reports and, upon request, shall make it available to the Financial Intelligence Unit or other relevant authority.
11. The CO shall inform the Employee on further steps to be undertaken in relation to the Client.

31. Reporting Procedure: External reporting

As already described in the previous section, the Compliance Officer shall receive and evaluate internal unusual transaction reports. He will open and maintain a log detailing the progress related to each report, noting down any information which needs to be documented so as to ensure that an adequate track record of the reasons leading to his decision are maintained. Such documentation may also be used to assist the Authorities in any analysis or investigation of the suspected money laundering, funding of terrorism, proliferation of WMD when such details are directly requested from the CO. This log shall be held by the CO and shall only be accessible to him, and will not form part of the Client's file. The CO shall gather all the necessary information and pose any questions to any of Company's employees as part of his investigation. The employees (whether those having submitted the internal report or otherwise) shall provide the CO with relevant information.

1. Once the CO decides that there are reasonable grounds which warrant the submission of a UTR the CO shall disclose that information, supported by the relevant identification and other documentation, to the FIU as soon as practicable, but not later than within 48 hours via the "GoAML" online portal and shall make a relevant record to the register of external suspicious transaction reports.
2. No copies of either the internal or external reports will be made. The CO will keep such records secure.
3. The CO shall, where appropriate, inform the originator of the internal report whether or not a formal disclosure has been made.
4. Following a formal disclosure, the CO shall take such actions as required by the Authorities in connection with the disclosure and accordingly follow their instructions.

Failure to report a suspected breach can result in the imposition of corporate and personal fines.

There are mandatory cases, when the Compliance Officer shall submit an Unusual Transaction Report (UTR) to the FIU Curacao based on the following objective factors:

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice
- Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- Transactions in the amount of XCG 5,000 or more regardless of the payment method used or be it a single transaction or a series, combination or pattern of transactions involving a total amount of XCG 5,000 or more and is considered per gaming day.

Therefore, the CO shall daily monitor such cases and report them to the FIU via goAML portal not later than within 48 hours.

32. Dealing with the requests from the Authorities

1. All the requests / inquiries from the Authorities must be deemed urgent.
2. The CO shall regularly review the goAML portal and ensure there are no undue requests / information inquiries from the FIU.
3. Such requests / information inquiries shall be replied as soon as possible, but not later than within 5 working days or as may be specified in the request.
4. The response shall be made by CO via goAML portal, if not specified otherwise by the FIU.
5. The CO shall create the Company's internal register of requests / information inquiries from the Authorities and log all such requests in it accordingly. The information in the register shall contain: the date and

reference number of the request, the date of response, the details of the person in question; any additional remarks.

6. The information in the request, as well as the information provided in terms of the response to the request, shall be deemed strictly confidential and shall not be disclosed to any third uninvolved parties.

Failure to comply with the reporting obligations can result in the imposition of corporate and personal fines.

33. Tipping Off

The offence of tipping off is committed by a person who discloses information that is likely to prejudice an actual or a proposed investigation. This can be either before or after an unusual transaction report is made to law enforcement, and includes circumstances where the offender knows or suspects that there is either an investigation or a proposed investigation or that a disclosure has been made to law enforcement. The offence is widely misunderstood. It is mistakenly assumed that enquiries should not be made of clients at the time that a concern is first developed for fear that such enquiries might expose an employee to tipping the client off. This is not the case. While enquiries must be handled with care, an employee will only be in danger of committing a tipping off offence if they either know that a report has been made or know that an investigation is underway or is planned. This should never be the case at the stage before a suspicion is formulated. Tipping off does, however, become a very real danger once a UTR is made to law enforcement, after which all communications between a company, its employees and suspected clients must be handled with care. All employees should look for guidance from either the Compliance Officer or from management on how to deal with suspected clients. It is also important to stress that the offence can be committed by communicating prejudicial information to people other than the suspect. Communications with representatives of suspected launderers, such as family members and lawyers, must also be treated in the same way. If the employee becomes suspicious about any transaction or activity of the client and intends to make inquiries to the client about such transaction or activity, ***the employee is not allowed to make any disclosures to the client about his suspicions, including informing the client about the following:***

1. That the client's account has been flagged or any transaction made by the client has in any way or for any reason been flagged or raised suspicions
2. That there is a possibility, that the information about the client could be notified to the supervisory or other relevant authorities
3. Any details of Compliance Officer

In case of any suspicions, even when those are not yet confirmed or filed internally or externally, the inquiries must be made in such a usual business correspondence manner, that the client could not understand or even have a hunch that the employee has any suspicions in respect of the client. Otherwise, such disclosures to the client are considered tipping off and so are an offence under AML Regulations.

Who the employees can talk to about any suspicion they have:

- ☐ The Compliance Officer is the first on the list. He will provide guidance on how best to proceed.
- ☐ It is allowed to discuss it with the senior manager, but it is in no case mandatory. There may be instances wherein the senior manager disagrees with the employee, but the employee still feels he has reasonable grounds to suspect wrongdoing. In such circumstances, the employee has to inform the Compliance Officer anyway about his suspicions.

Making routine commercial enquiries of a client is acceptable as this may actually remove any suspicion the employee has. Again, this must be sensitively handled under direction from the Compliance Officer.

It is important to note that tipping off can become a risk when terminating a Client's account for reasons relating to suspicion of money laundering or terrorist financing. In such cases, the Company must ensure that no explicit indication is given in any message conveyed to the Client that suspicion of money laundering or terrorist financing exists. Instead, communications regarding the termination of the account should be kept general. The Compliance Officer can provide guidance on such communications.

34. Training

Recruiting staff of integrity is not sufficient. Staff must have sufficient awareness and training to detect money laundering, terrorist financing and proliferation of WMD and to understand what is expected of them.

It is essential for the effective ML/FT/PF risk management that:

- ☐ Employees have sufficient knowledge and awareness to detect money laundering / terrorism financing/ proliferation of WMD.
- ☐ Employees have sufficient training to know how to deal with cases once they know of or suspect money laundering or terrorism financing.
- ☐ Employees have knowledge on how to act in cases when the client appears to be a sanctioned person
- ☐ Employees are aware of their personal legal obligations and rights.

The training plan shall be developed at the beginning of each financial period and approved by the Compliance Officer or senior management. The said training plan shall at least include the following information: the dates, topics, training provider, indication whether the training is internal or external, employees, who shall attend the training.

Training must be provided to all employees (new and existing). The new employees shall have induction training before they proceed to execute their responsibilities, but at maximum within 3 months after employment to a relevant job function. The trainings at a minimum must include:

- ☐ General nature and process of ML/FT/PF
- ☐ AML/CFT/CPF Policies and procedures of the Company;
- ☐ AML/CFT/CPF Regulatory obligations of the Company
- ☐ CDD / EDD procedures;
- ☐ Instructions on how to act in cases of PEP/Sanctioned Individual Status of a Client;
- ☐ Reporting obligations;
- ☐ Signs and examples of suspicious activities;
- ☐ Analysis of Client's transaction patterns;
- ☐ Recognition and handling of operations and transactions which may be related to proceeds of criminal activity, money laundering, the funding of terrorism, proliferation of WMD.
- ☐ Record keeping obligations and data security

Additional training should be provided regularly to all employees based on, but not limited to, changes in government regulations, changes to the requirements in the Company's AML/CFT/CPF Policy and relevant procedures.

All training sessions must be documented and retained with the Training Log by the Compliance Officer.

Training Log shall contain the following information:

- Details on the actually received content of the training programs;

- The names of the staff members/departments who have received the training;
- The date on which the training was provided;
- The results of any testing or other type of verification carried out to measure staff understanding of ML/FT/PF

An employee should also receive additional AML training in the event of a performance issue related to an AML incident.

AML/CFT/CPF refresher training will be delivered at least annually for all staff.

The Compliance Officer will provide additional and up-to-date information such as amendments to legislation, emerging risks and suspicious transaction / activity typologies and any other important industry-specific developments related to the AML/CFT/CPF field.

35. Staff recruitment

It is important that the Company takes appropriate steps to ensure the integrity of its new employees. Such steps should be risk based, with the extent of the effort proportional to the role of the employee and the money laundering threat inherent to the role they are being recruited for.

The following staff screening procedures shall be operated by the Company:

- ☐ At least one reference letter shall be requested for senior level employees.
- ☐ Copies of relevant qualifications will be obtained when requesting sight of certificates. Copies of such certificates will be retained on the employee's file.
- ☐ Curriculum Vitae will be obtained from the prospective employees. The employment history included on the CV will be tested by taking a reference from a previous employer. This should usually be the most recent employer.

For the staff recruited for Manager, Compliance Officer or Director positions, the following additional checks shall be performed:

- ☐ The identity of the prospective employee shall be verified by requesting sight of identity verification documents.
- ☐ A non-conviction certificate issued by the police / Ministry of Internal Affairs shall be required to be provided

All the Company's employees have signed the employment agreements that contain non-disclosure conditions to maintain confidential sensitive data they deal with. Any case of serious violation of the AML/CFT/CPF policies and procedures can be a sufficient reason for termination of employment.

36. Staff Responsibilities

All staff is required to:

1. At all times comply with the Company's AML/CFT/CPF Policies, Procedures and other internal control systems, including all measures relating to anti-money laundering, counter terrorist financing and proliferation of WMD procedures;

2. Disclose any suspicion of money laundering, terrorist financing, proliferation of WMD to the Compliance Officer.

37. Record Keeping

The Company shall maintain appropriate records of all the Clients and their associated transactions for the purposes of ML/FT/PF risk management and the prevention, detection, analysis and investigation of money laundering; funding of terrorism or proliferation of WMD activities by the supervisory authorities.

Records shall be maintained in electronic format in a secure manner and shall be access-controlled.

The following records shall be retained:

- 1) The list of all business relationships setting out:
 - ☐ Full name of the Client and/or Client reference number
 - ☐ the type of service being provided, or product being offered
 - ☐ the date of commencement of the business relationship and, where applicable, the date on which it ceased
 - ☐ whether the Client is a PEP / a Family member of a PEP / a Close Associate of a PEP;
- 2) Customer Due Diligence documentation, data and information;
- 3) Records necessary to reconstruct all transactions carried out by the client;
- 4) Register of internal reports of unusual transactions (Register of Internal Unusual Transaction Reports), including a record of any written determinations made;
- 5) Register of any disclosures made to the FIU (Register of External Unusual Transaction Reports)
- 6) Records of any training provided to the employees;
- 7) Records of internal and external reports filed
- 8) All the correspondence with the Client

The above-mentioned records shall be kept for the period of 5 years, starting from the date when the business relationship ends.

For the registers of internal and external UTRs the period of 5 years starts on the later date choosing between the date of end of business relationship or the date when the report was submitted.

As for the training records, the period of 5 years starts on the last day of the training conducted.

The period of five years may be extended, where such extension would be considered necessary by the relevant authorities.

The records shall be made available to the relevant authorities for the purposes of the prevention, detection, analysis and investigation of money laundering, the funding of terrorism or proliferation of WMD upon their request.

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

The records shall be kept in a secure manner and used only for legal and/or regulatory obligations, which the Company is subject to. The Company applies all the necessary technological tools, to ensure data security. The Company's Privacy Policy serves as a main document to inform the Clients about their data security and the purposes for which it is stored.

The Employees shall not request the Clients to provide the documents, that would be irrelevant, or which do not contain any essential or valuable information, which would help the Company to comply with the AML Regulations.

It is an offence to make use of any personal details of the Clients, including the obtained CDD documentation, information and data, for the purposes other than those to comply with the Company's legal and/or regulatory obligations without client's permission to do so.

38. Funds Management procedure and Pay-out of gambling winnings

1. The Company shall accept only those Client deposits, which are made from accounts held with licensed financial institutions or licensed payment providers.
2. The Company does not affect any cash deposits or withdrawals in any case.
3. Funds may be received from the Clients only by any of the following methods: credit cards, debit cards, electronic transfer, wire transfer cheques and any other method approved by the Company or respective regulators. The funds deposited by the Client along with any bonuses, winnings or other loyalty rewards provided by the Company shall be credited to the corresponding Client's gaming account.
4. The Company shall accept only those payment methods, which belong to the Client and not to any other third party. Where there are doubts about the funding method, verification documents to confirm that the payment method belongs to the Client shall be requested.
5. The funds deposited by the Client and/or winnings due to a Client from his online account can be paid only:
 - ☐ To a payment method from which a deposit has previously been made by the Client and which the Company is satisfied still belongs exclusively to the Client; In cases when the above option is impossible, then the Company will formally request for Client verification documents and also request for details of another payment method that may be confirmed to be in the Client's name and hence minimising the risk of remitting funds to an individual that is different from the person that had originally remitted the deposits. This process is in place to among other purposes discourage credit card theft and identity theft.
 - ☐ When it is ensured that the institution to which the funds are to be remitted is situated in a reputable jurisdiction and/or has equivalent AML/CFT/CPF requirements as are applicable to the Company. Obviously enough this also ties in to the institutions from where Client deposits are accepted.
6. Before processing any withdrawal request made by the client, the employees shall ensure that the Company is in possession of information and / or documents required from a client and the CDD procedure has been successfully completed, where applicable. The transactions are analysed on the aspects of possible fraud / ML / FT/ PF, gaming activity before paying the funds out.

7. In any case, before any withdrawal, regardless of the amount involved, the Client has to provide at least the identity confirming document, examples of which are provided in Section 17 of this procedure.

Other fraud management tools used by the Company:

- ☐ Automatically flagging those Clients in the System, who request withdrawal without sufficient gaming activity.
- ☐ Geo-location System and IP monitoring tools allow to review the IP address of the Client, including from where the account has been registered or accessed; each access is being logged.
- ☐ Closed loop payments – the Clients are automatically rejected to withdraw funds to the payment method, different from that, which was used for making deposits. If still required, the Client needs to contact the employees of the Company.

Same credit card but different Clients situations

The Company does not accept payments from / to third parties. So, the Client is only allowed to use the payment method that belongs to him. Credit cards under third party names are not accepted.

Same Client, but different credit cards situations

The employee must ensure that the payment method belongs to the Client in question. Payment methods belonging to a different person, shall not be accepted.

Also, the employees shall be regularly reminded by the Compliance Officer, that if the client uses multiple payment methods, in particular within a short period of time, such Client's behavior could lead to suspicion of fraud. Therefore, the employees shall be vigilant at all times, where necessary, require the proof of payment documents or file UTR to the Compliance Officer, if it is deemed necessary.

Inconsistencies in IP locations

The following data available in the Client's Profile is being cross-referenced: the residential address indicated by the Client at registration, the actual registration IP and the IPs from where the account is being accessed. The cases of any major inconsistencies (e.g., the Client indicated his residential address in Brazil, however, the actual account access IP is in India; or access from multiple IPs to one and the same account has been registered) shall be questioned, if necessary escalated to the senior manager or Compliance Officer. The employee also needs to consider filing of internal UTR, where necessary.

39.Fictitious, Anonymous & Multiple Accounts (fraud management)

The Company shall not set up Client accounts which are anonymous or there is knowledge or reasonable grounds to suspect that the details provided by the individual are fictitious.

As described above, any transfers of funds between the Clients are prohibited.

Where it is determined that the Client attempted to register an account with fictitious details (e.g., during CDD procedure, it is established that the Client's registration details contained in his profile and details in the provided ID document are completely different), the account of the Client shall be blocked, and the Employee shall file the internal unusual transaction report for consideration of the Compliance Officer.

The employees also monitor cases, where clients are suspected to register multiple accounts linked to one individual.

The System has the feature "Duplicate level", which shows user parameters that coincide with parameters of other Company's clients. The following parameters are being checked during the verification of account duplication:

- ☐ **E-mail** - e-mail duplication is checked. Check is performed up to @ or + sign;
- ☐ **Password** - password uniqueness is checked. If two different users have the same password, then it is considered to be duplication;
- ☐ **IP** - registration IP's are checked for duplication;
- ☐ **Browser** - every browser has its own unique identifier. Thus, uniqueness of those identifiers is checked;
- ☐ **Last Login IP** - IP + Login pair is checked. If user logged in with different logins from one IP, this IP is considered to be duplicate;
- ☐ **Payer ID** - user address, wallet or credit card ID is checked;
- ☐ **IBAN** - user IBAN is checked for duplication.

The Company shall not register the accounts, where:

1. The e-mail of a Client has already been registered with the Company

Other cases of potential multiple accounts shall be analysed in a case-by-case manner, taking into consideration the following:

- ☐ which and how many parameters are identical
- ☐ are the parameters in fact identical or those contain only small identical part?
- ☐ other information provided by the Clients during CDD/EDD procedure

Such accounts are subject to more closer monitoring and verification by the Employees. Where suspicions about fraud arise, such cases must be escalated to the Compliance Officer and the accounts are considered to be blocked.

40. Reliance on Third Parties

The Company does not rely on any third party for performing its customer due diligence measures.

41. Business Risk Assessment

The Company has developed and documented the Business Risk Assessment (BRA), displaying the Company's potential vulnerabilities in terms of AML/CFT/CPF and Sanctions risk management. The BRA contains the detailed assessment of the likelihood and the impact on the Company's business, if risk factors materialize; as well as measures and controls applied by the Company to mitigate those risks. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services and products provided by the Company, the Clients to whom services are offered, transactions performed by these Clients, delivery channels offered by the Company, the geographic locations of the

Company's clients and other qualitative and emerging risks. When developing BRA, both national and supranational risk assessments are considered, such as for example Curacao National Risk Assessment⁴.

The identification of AML risk categories is based on the Company's understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.

The Business Risk Assessment shall be reviewed and/or updated whenever there are changes to the environment within which the Company operates and within its business activities, such as introduction of new payment methods, new markets, new games or regulatory changes. In the absence of changes, the Company shall review and/or update the BRA at least annually. The BRA shall be approved by the Board of Directors of the Company and made available to the supervisory authorities upon request.

42. Technological Developments Risk Assessment

The Company shall perform additional ML/FT/PF risk assessment whenever:

- A new product is developed;
- A new business practice emerges;
- A new delivery mechanism becomes available;
- A new or developing technology is used for both new and pre-existing products.

Where the risks are identified, relevant mitigating measures and controls shall be described and implemented.

Such risk assessment shall be performed prior to launch of the new products, business practices, delivery mechanism or the use of new or developing technologies

43. Internal Controls and Compliance

The Internal Controls are developed and Compliance procedures for monitoring and testing compliance with the AML/CFT/ CPF legislation are regularly conducted to ensure that:

- ☐ Risks are properly identified and documented
- ☐ The operational performance of such risks is monitored
- ☐ Prompt action is taken to remedy any deficiency
- ☐ A report is submitted to senior management at least annually, describing:
 - Company's AML/CFT/CPF environment including developments in relation to new legislation
 - Progress on internal developments in relation to Company's policies, procedures and controls for AML/CFT/CPF.

The Compliance Officer shall regularly, at least twice a year or more often, if deemed necessary, engage in compliance tests in order to be assured that the Company's AML/CFT/CPF Policies and Procedures are functioning properly. The said Compliance tests should involve the following activities:

- 1) Asking employees about their duties
- 2) Observing employees in the conduct of their duties

⁴ <https://minfin.cw/wp-content/uploads/2023/05/Publieke-Versie-NRA-Curacao-2020.pdf>

3) Reviewing documentation to see if procedures have been followed

The results of each compliance test shall be properly documented and reported to the senior management. The results shall also be kept for the provision to the Supervisory Authorities upon their request.

The Company will take active measures to monitor operational compliance with the AML / CFT / CPF policies and related procedures. The Compliance Officer will be responsible for setting the framework and will provide routine reports to Management on the effectiveness of the procedures being implemented across the Company. Where applicable, actions will be taken to rectify any perceived shortcomings and appropriate training on procedures will be provided to the employees within their roles to help provide a robust and effective framework for AML / CFT within the Company.

To ensure that the Company's internal controls are effective at all times, the adopted risk management measures remain adequate and the emerging risks are considered in a timely manner, the Compliance Officer shall regularly review relevant information sources, such as the results of the national and supranational ML/FT/PF risk assessments, guidelines issued by FATF, by the FIU, or other relevant authority or information obtained as part of the CDD process. This shall involve, in particular:

- ☐ Regularly reviewing media reports that are relevant to the gaming sector or jurisdictions in which the Company is conducting its business
- ☐ Regularly reviewing law enforcement alerts and reports
- ☐ Ensuring that the Company becomes aware of changes to terror alerts and sanctions regimes as soon as they occur, for example by regularly reviewing terror alerts and looking for sanctions regime updates or subscribing to receiving updates from the relevant authorities, where possible
- ☐ Regularly reviewing thematic reviews and similar publications issued by competent authorities.

44. AML Compliance Program

The Company has developed the AML Compliance Program to meet its objectives and be in full compliance with the Curacao laws and regulations.

The following elements of the Compliance Program have been implemented:

- 1) The Compliance Officer has been appointed to constantly monitor and update if needed the AML Compliance Program
- 2) The policies, procedures and controls have been developed to ensure compliance with the laws and regulations
- 3) The employees screening program is applied and employees receive necessary induction and regular refresher trainings
- 4) AML program is regularly, but at least annually, tested by the independent internal audit to assure compliance with AML regulations

At least the following compliance tests shall be performed during annual independent internal audit:

- An evaluation of the Company's AML/CFT/CPF policies and procedures;
- 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.

The scope and results of the testing shall be documented and reported to the Compliance Officer and the Board of the Directors. Where deficiencies were identified, the internal auditor shall recommend corrective actions, which shall be implemented by a certain deadline. These corrective actions could also include enhancement of controls and procedures.

45. Policy Breaches And Disciplinary Actions

Non-compliance with the legal and regulatory obligations may result in administrative and criminal sanctions imposed on the Company, which may entail large financial losses, reputational damages, penalties and even license suspension or revocation. Therefore, non-compliance with this AML/CFT/CPF Policy and procedures, including amongst others failure to adhere to verification, monitoring, AML, data security, or fraud prevention protocols, may result in disciplinary action, such as warning, mandatory re-training, enhanced performance monitoring, demotion or role change or even up to termination of employment.

Any violations identified during internal audits, transaction monitoring, or regulatory reviews are escalated to the Compliance Officer, which assesses and enforces appropriate remedial actions.

The CO is responsible for ensuring all breaches are documented and corrective measures are implemented.

Repeated offenses or significant breaches may lead to further legal action or sanctions, depending on the severity of the violation.

46. Policy Revision

The AML / CFT / CPF Policy and related procedures are subject to review, update and amendments by the Compliance Officer, taking into consideration the latest amendments to Curacao legislation, forecasting potential new risks related to changes in Company's product / service range and volume, new product / service promotion, new technological developments implementation, business geographical changes, as well as other newly discovered risks. In any case, the AML / CFT / CPF Policy and related procedures are subject to review and/or update at least annually. The Company shall ensure external independent review of its AML /CFT/CPF policies and procedures in urgent situations, such as essential changes in AML/CFT/CPF legislation.

47. Annex 1: Indicators of Suspicious Activity of Money Laundering / Terrorist Financing

Money laundering indicators related to identifying the person

1. When opening an account, the client refuses or tries to avoid providing information required, or provides information that is misleading, vague, or difficult to verify.
2. Identification presented by the client cannot be verified.
3. Inconsistencies in the identification documents or different identifiers provided by the client.
4. Client produces seemingly false information or identification that appears to be counterfeited, altered or inaccurate.
5. Client alters the transaction after being asked for identity documents.
6. The client provides only a non-civic address such as a post office box or disguises a post office box as a civic address for the purpose of concealing their physical address.
7. Transactions involve individual(s) identified as being linked to criminal activities.
8. The Client in fact acts on behalf of a third party, not on behalf of himself as declared.

Money laundering indicators related to client behaviour

1. Client exhibits nervous behaviour or has a defensive stance to questioning.
2. Client presents confusing details about the transaction or knows few details about its purpose.
3. Client avoids contact with Company's employees or refuses to provide information.
4. The client refuses to identify a source of funds or provides information that is false, misleading, or substantially incorrect.
5. Client closes account after an initial deposit is made without a reasonable explanation.

Money laundering indicators surrounding the financial transactions in relation to the person profile

1. The transactional activity is inconsistent with the client's apparent financial standing, their usual pattern of activities or occupational information.
2. Client appears to be living beyond their means.
3. Large and/or rapid movement of funds not commensurate with the client's financial profile.

Money laundering indicators related to products and services

1. Use of multiple foreign bank accounts for no apparent reason.
2. Use of multiple payment methods for no apparent reason.
3. Credit card transactions and payments are exceptionally high for what is expected of the client.

Money laundering indicators related to transactions structured below the identification requirements

1. Client appears to be structuring amounts to avoid identification thresholds.
2. Client appears to be collaborating with others to avoid identification thresholds.

The ML/TF indicators specified by Asia/Pacific Group on Money Laundering⁵:

⁵ <https://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf>

1. Frequent deposits into casino account without reasonable explanation.
2. Funds withdrawn from account shortly after being deposited.
3. Account activity with little or no gambling activity.
4. Player account transactions conducted by persons other than account holder.
5. Associations with multiple accounts under multiple names.
6. Client requests to transfer funds into third party accounts.
7. Client requests to transfer funds from player's account to a charity fund.
8. Structuring of deposits / withdrawals or wire transfers.
9. Attempting to use third parties to undertake wire transfers and structuring of deposits.
10. Use of multiple names to conduct similar activity.
11. Use of player's account as a savings account.
12. Activity or income is inconsistent with the Client's profile.
13. Client name and name of account do not match.
14. Requests for casino accounts from Politically Exposed Persons (PEPs).
15. Noticeable spending / betting pattern changes.
16. Clients depositing large deposits but play the games that have high payout percentages (or low volatility games) and do not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play.
17. Client's intention to win is absent or secondary.
18. Client befriending/attempting to befriend casino employees.
19. High volume of transactions within a short period.
20. Multiple withdrawal requests within the same day.
21. Requests for credit transfers to other casinos.
22. Unexplained income inconsistent with financial situation/Client profile.
23. Dramatic or rapid increase in size and frequency of transactions for regular account holder.

Structuring or „smurfing“ involves the distribution of a large amount of funds into a number of smaller transactions in order to minimize suspicion and evade threshold reporting requirements. Common methods of structuring include:

- ☐ Regularly depositing or transacting similar amounts of funds, which are below a country's reporting disclosure limit.
- ☐ The use of third parties to undertake transactions using single or multiple accounts.
- ☐ Regularly switching gaming accounts within a chain when the wagering amounts are approaching the reporting threshold.
- ☐ Requesting the division of winnings, which exceeds the reporting threshold, to be broken down into funds to be withdrawn below the reporting threshold.

ML/TF Indicators associated with the use of Virtual Assets (VA):

- ☐ Client conducts activities with VA, whose public key is related to black market purchases (Darkweb) or other illegal activity
- ☐ Client VA public key is disclosed on websites that are associated with illegal activities
- ☐ An analysis of the blockchain clearly shows that the virtual wallet has a suspicious source of funds, such as that related to black market purchases

- The Client's email address or phone number is associated with a recognizable VA peer to peer exchange platform for its advertising purposes
- Client's VA transactions are made from questionable IP addresses, from IP addresses registered in sanctioned countries, or from IP addresses identified as suspicious
- A Client, who is significantly older than most users of a VA platforms, opens a VA account and conducts a large amount of different transactions, raising suspicions, that a money mule is involved in the transactions, or an older person has become a victim and is being used to commit criminal activity
- The Client has poor knowledge of VA transactions despite being involved in VA transactions (this could indicate that the person is a victim of fraud and may be used for ML/TF operations)
- In VA transactions mixing and tumbling services are applied, indicating the intent to hide illicit money flow between the virtual wallet and black market
- Client redirects a large number of VA transactions to VA platforms registered in low-tax or tax-free countries and territories
- Structuring VA transactions (e.g., exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions –
 - in short succession, such as within a 24-hour period;
 - in a staggered and regular pattern, with no further transactions recorded during a long period afterwards; or
 - to a newly created or to a previously inactive account
- Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where –
 - there is no relation to where the customer lives or conducts business; or
 - there is non-existent or weak AML/CFT regulation
- Depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.
- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency.

Information Sources:

- 1) FATF Report on Vulnerabilities of Casinos and Gaming Sector
- 2) FATF Report on Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing

48. Annex 2: Examples of documents, that can prove client's source of funds/wealth

The type of source of funds	Examples of confirming documents
Employment	One of the following: ☐ Reference letter, issued by the employer, showing the duration of cooperation (not less than 3 months), the job position, the salary of the employee and the details of the employer ☐ Bank statement, showing regular incoming salary payments from the employer ☐ Reference from the tax authority / income tax return ☐ Payslips from the employer
Inheritance	1) The Will or Grant of Probate 2) Certified letter from the licensed solicitor / trustees / executor
Gift	1) Documentary evidence of the donor's source of wealth (as detailed in this table); 2) Bank statement confirming proceeds received or other documentary evidence shall be required to support this (depends on the gift or donation); 3) Gift agreement
Loan	1) Loan agreement, supported by the bank statement confirming receipt of the loan. Loan agreement should contain at least the following information: purpose, re-payment schedule, full details of the lender and the borrower, details of the dispute settlement procedure by the parties If the loan is issued by the third party, and not by the bank, documentary evidence of the lender's source of funds and source of wealth must be provided
Receipt of dividends	1) Audited financial statement of the company, showing the dividend distribution 2) Bank statement showing the incoming payment / dividends distribution 3) resolution by the shareholders for the dividend distribution
Maturity of life policy	1) Life policy; 2) Closing statement clearly indicating closing amount and name of client;

	3) Bank statements clearly showing receipt of pay-out and name of insurance company.
Sale of Investments	1) Investment/savings certificates, contract notes; 2) Bank statement clearly showing receipt of funds and name of investment company; 3) Letter detailing receipt of funds from a regulated accountant or regulated broker.
Property Sale	1) Sales contract (copy of original document or a duly certified copy); 2) Proof of receipt of funds, e.g. bank statement; 3) Letter from a licensed solicitor or regulated accountant, stating property address, date of sale, proceeds received, and name of purchaser; 4) 4. Extract from official Real Estate register.
Company / Business sale	1) Contract of sale (copy of original document or a duly certified copy); 2) Bank statement confirming proceeds received; 3) Letter detailing company's sale signed by a licensed solicitor or regulated accountant; 4) Documents confirming the client's ownership of the sold company; 5) Verifying the ownership and transfer of the ownership of the company accordingly via official register of enterprises.
Divorce settlement	1) Court order; 2) Letter detailing divorce settlement, as well as clearly indicating the amount of settlement, signed by a licensed solicitor or advocate.
Deposits / savings	1) Documents of how the savings were acquired (as detailed in this table); 2) Savings statement clearly showing name of client and amount of funds.
Lottery or gambling win	1) Evidence from the lottery company; 2) Cheque/Winnings' receipt.
Retirement income	One of the following: 1) Pension statement clearly showing name of provider, name of client, amount and frequency of income; 2) Bank account statement showing name of pension provider, name of client and receipt of pension income.

Company / Business profits	One of the following: 1) Copy of latest audited financial statement; 2) Documentary evidence of the nature of business activity and turnover – contracts, invoices, transportation documents, bank statements confirming proceeds received, etc.
----------------------------	---

49. Annex 4: KYC questionnaire for natural persons

This KYC Questionnaire is developed for the purpose of Company's compliance with the AML Regulations of Curacao. Therefore we kindly ask you to provide the answers to the questions below.

Personal Details of a Customer

Full name:
Date of birth:
Nationality:
Current residential address:

Business / Occupation / Employment details

☐ If Self-employed, please specify the following details:

Company name:
Registration number:
Registered address:
Place of business, if different from the registered address:
Industry:

☐ If employed, please specify the following details:

Occupation:
Company name:
Registration number:
Registered address:

☐ Other (please give details):

The expected source and origin of the funds to be used throughout the business relationship:

☐ Salary	☐ Business profits
☐ Dividends	☐ Proceeds from investment activity
☐ Sale of assets (please specify)	☐ Gift
☐ Inheritance	☐ Other (please specify) _____

Gross annual income (Euro):

☐ less than 10,000	☐ 50,000-100,000
☐ 10,000-50,000	☐ More than 100,000

Expected nature and purpose of the business relationship with the Company

Planned monthly deposit amounts (Euro)

☐ Less than 5,000	☐ 50,000-100,000
☐ 5,000 – 10,000	☐ More than 100,000
☐ 10,000-50,000	

Please put a tick in a box below only if a statement is applicable to you:

☐ I am the sole beneficial owner of the player's account established with the Company and do not represent or act on behalf of any third party

Please indicate if you are a PEP / a Family Member of a PEP / Close Associate of a PEP:

☐ Politically Exposed Person⁶

☐ A Family Member of Politically Exposed Person⁷

☐ A close Associate of Politically Exposed Person⁸

I hereby confirm that the information provided herein is accurate, correct and complete and I undertake to inform the Company in writing of any changes to the information already provided and to update the information on this form whenever requested to do so by the Company. I am aware that it is an offense to deliberately provide false and / or misleading information.

Date:

Customer's signature:

⁶ "politically exposed persons" means natural persons who are or have been entrusted with prominent public functions in or outside Curacao, such as but not limited to Heads of State / Government, Ministers, Deputy or Assistant Ministers, Parliamentary Secretaries, Members of Court, Ambassadors, Members of the administrative, management or supervisory boards of State-owned enterprises (other than middle ranking or more junior officials)

⁷ the spouse, or a person considered to be equivalent to a spouse/ the children and their spouses, or persons considered to be equivalent to a spouse / the parents of a PEP

⁸ a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement, or any other close business relations, with that PEP or a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP

50. Annex 5: List of links to public registers

Country	Link to public register of legal entities / private entrepreneurs
UK (PSC details must be filed for all LPs and LLPs)	https://beta.companieshouse.gov.uk/
Ireland	https://search.cro.ie/company/CompanySearch.aspx or https://www.cro.ie/Publications/LTD-Partnerships
Malta	https://registry.mbr.mt/ROC/index.jsp#companySearch.do?action=companyDetails
Latvia (Authentication is available via online banking to get more info about the client, incl. Financial Statements)	https://info.ur.gov.lv/#/data-search
Estonia	https://ariregister.rik.ee/
Lithuania No official public register available. For some details visit the website indicated in the next column	https://rekvizitai.vz.lt/
Germany Information is available only after purchase	https://www.unternehmensregister.de/ureg/ ; or https://www.handelsregister.de/rp_web/mask.do?Typ=n
Switzerland (info about the shareholders is not available)	https://www.zefix.ch/en/search/entity/welcome
Slovakia	http://www.orsr.sk/search_subjekt.asp
Slovenia	https://www.ajpes.si/prs/default.asp
Finland	https://tietopalvelu.yti.fi/yrityshaku.aspx?kielikoodi=3
Portugal	http://publicacoes.mj.pt/Pesquisa.aspx
Hungary	https://www.e-cegjegyzek.hu/?cegkereses
Bulgaria	https://portal.registryagency.bg/CR/Reports/VerificationPersonOrg
Cyprus (info about the shareholders is not available)	https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchForm.aspx?sc=0
Poland	https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/index.html
Denmark	https://datacvr.virk.dk/data/index.php?q=forside&language=en-gb
Czech Republic	https://or.justice.cz/ias/ui/rejstrik
Canada	https://beta.canadasbusinessregistries.ca/search
Hong Kong	https://www.icris.cr.gov.hk/csci/
Singapore	https://www.tis.bizfile.gov.sg/ngbtisinternet/faces/oracle/webcenter/portalapp/pages/TransactionMain.jspx?selectedETransId=dirSearch&prchseInfo=BP#!%40%40%3FselectedETransId%3DdirSearch%26prchseInfo%3DBP%26_adf.ctrl-state%3D1cm03dhprk_8
Georgia	https://www.my.gov.ge/ka-ge/services/6/service/179

51. Annex 6: Internal Unusual Transaction Report

Internal Unusual Transaction Report

Specific to Employees to be submitted to the Compliance Officer for completion of the form:

It is your legal duty and a requirement of your employment with this practice that you report any knowledge or suspicion concerning money laundering to the Company's Compliance Officer.

In accordance with our internal procedures, you need to complete the report form as quickly as is practical. Should any delay be likely you need to contact the Compliance Officer immediately.

Please do not take any copies of this form.

Tipping off is a criminal offence. You should therefore avoid discussing your suspicions or concerns with anyone other than the Compliance Officer in all but the most unusual circumstances.

Failure to comply with these requirements may result in action being taken against you in line with the Company's usual disciplinary procedures.

To: The Compliance Officer
Date of the report: [Insert date]
Prepared by: [Insert name and position]
Name of individual(s) suspected: [Insert name of all individuals suspected]
Name of Customer (if different): [Insert Customer name or confirm that no difference from the list above]
Reason for suspicion: [Give a detailed description of the reasons for your knowledge or suspicions]
Date suspicion first aroused: [insert date]
Names of all other colleagues who have been involved with this Customer's affairs: [Insert name of all individuals informed – each of whom should sign the declaration below]

Declaration

I am aware of the risks and penalties regarding “tipping off”, or investigation of the above or related matters by the authorities.

Name:

Signed:

Dated