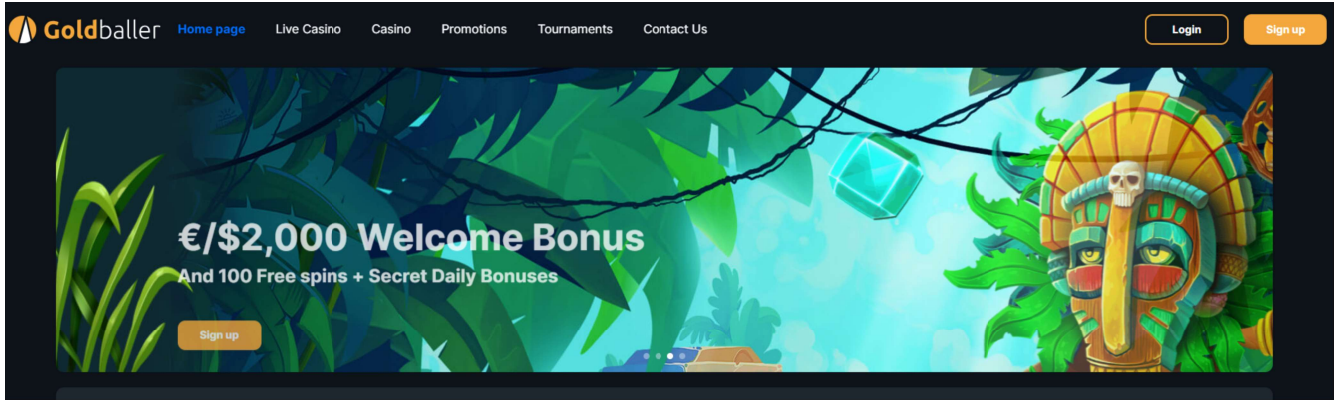
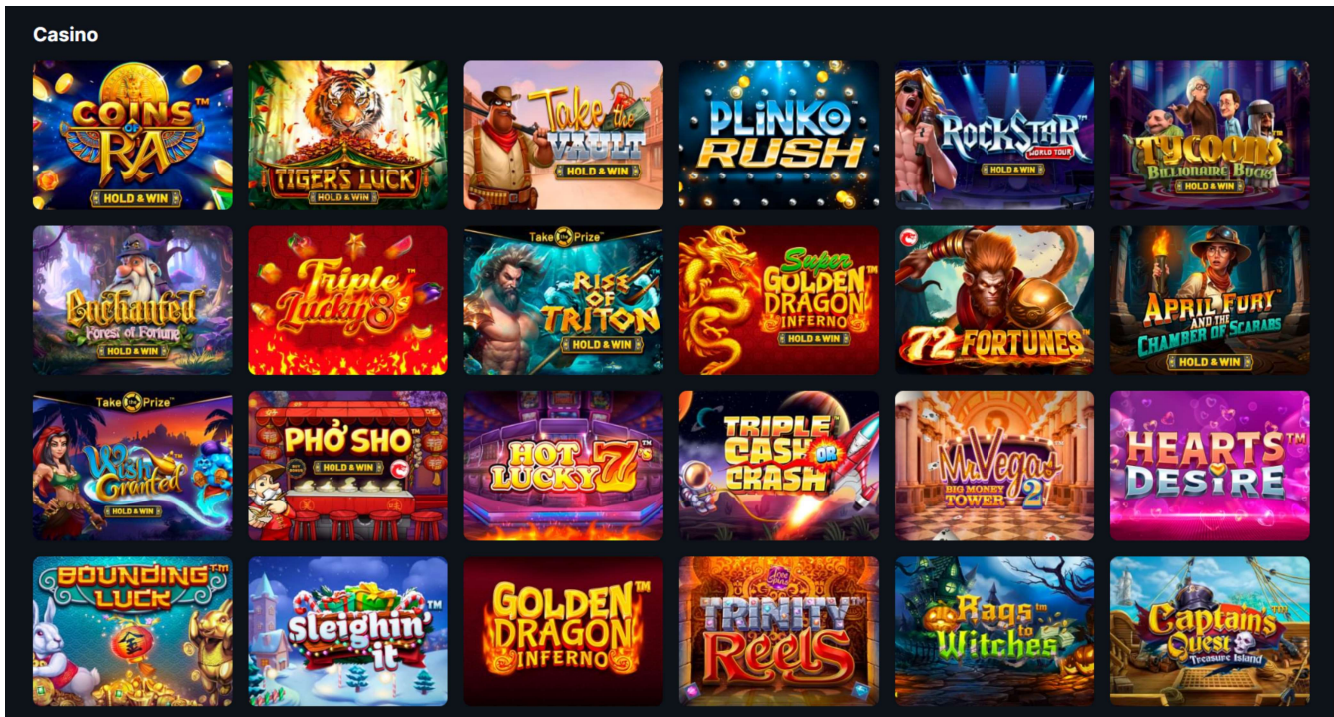




www.goldboller.com



Business Plan

Alisium B.V.

28.03.2024.

Overview of the business, software and company structure

Alisium B.V. (reg.no. 161507) is a Curacao established company in August 2022 under the Directorship of Morganite Corporate Services B.V. with a domain goldballer.com that operates under the Master License of Gaming Curacao with a software from BROMSTON ASSOCIATES LTD (Cyprus) and is a start-up project that was not launched till now. The UBO, CEO and founder of the Company/ Project is Mr. Maksims Rutenbergs with strong gambling operating and management skills, who is also a UBO of another gambling company SG International N.V. The history of his previous roles below:

16/08/2019 – current

COMPANY OWNER – COWORK SPACE OU (Estonia)

The field of activity of the company work with real estate on the co-work system

03/08/2022 – current

COMPANY OWNER – Alisium B.V. (Curacao)

Gambling start-up company

01/05/2012 – 14/07/2017

DIRECTOR OF ACCOUNT MANAGEMENT – CASINO EUROPA (Latvia)

Manage a team of Account Managers to drive revenue and exceed targets within existing and new business:

Create marketing strategy

Build and manage a leading team of Account Mangers, Sales and Marketing team.

Control, own and maintain marketing P&L

Monthly reporting and analytical analysis to management

Drive the sales marketing towards suppliers.

01/03/2012 – 01/10/2012

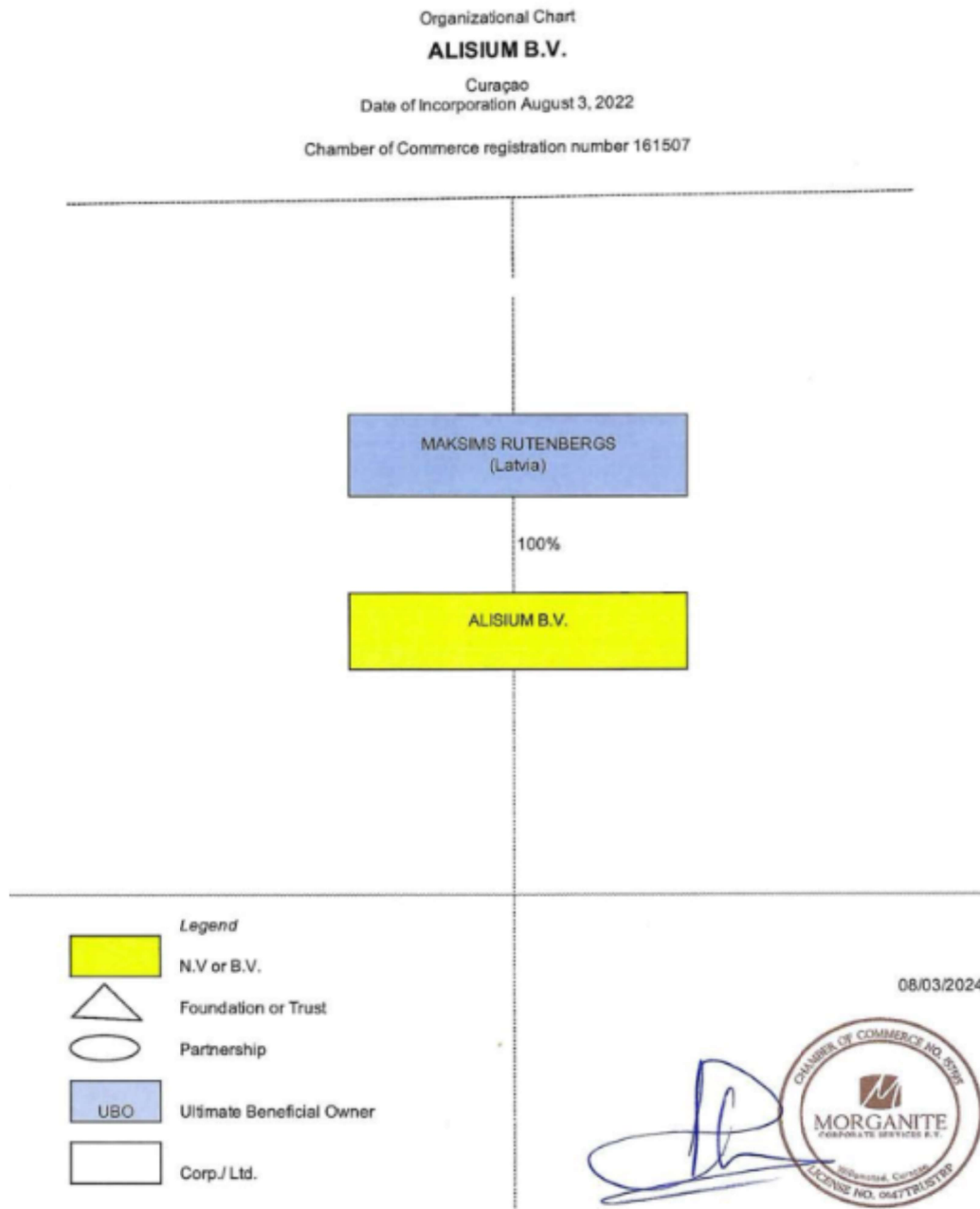
SENIOR ACCOUNT MANAGER – CASINO XO (Moldova)

Portfolio management

Building strong customer relationships

Developing account management strategies

Coordination of work of internal casino teams



Financial projections for 3 years

Expected Initial Investment (Financed by shareholder – as a start up): 100 000 EUR

2024/2026	Monthly revenue (EUR)	Commissions paid to contend providers	Commissions paid to platform providers	Project Marketing expenses	Other expenses	Monthly expenses total (EUR)	Profit/Loss (EUR) before Taxes
January,	€0	€0	€0	€0	€2,000	€2,000	-€2,000

2024							
February, 2024	€0	€0	€0	€0	€2,000	€2,000	-€2,000
March, 2024	€0	€0	€0	€0	€2,000	€2,000	-€2,000
April, 2024	€0	€0	€0	€0	€4,000	€4,000	-€4,000
May, 2024	€0	€0	€0	€0	€4,000	€4,000	-€4,000
June, 2024	€9,286	€1,857.14	€2,136	€15,079	€929	€20,000	-€10,714
July, 2024	€32,857	€6,571.43	€7,557	€17,586	€3,286	€35,000	-€2,143
August, 2024	€56,429	€11,285.71	€12,979	€30,093	€5,643	€60,000	-€3,571
September, 2024	€80,000	€16,000.00	€18,400	€47,600	€8,000	€90,000	-€10,000
October, 2024	€103,571	€20,714.29	€23,821	€40,107	€10,357	€95,000	€8,571
November, 2024	€127,143	€25,428.57	€29,243	€47,614	€12,714	€115,000	€12,143
December, 2024	€150,714	€30,142.86	€34,664	€60,121	€15,071	€140,000	€10,714
January, 2025	€174,286	€34,857.14	€40,086	€64,486	€17,429	€156,857	€17,429
February, 2025	€197,857	€39,571.43	€45,507	€73,207	€19,786	€178,071	€19,786
March, 2025	€221,429	€44,285.71	€50,929	€81,929	€22,143	€199,286	€22,143
April, 2025	€245,000	€49,000.00	€56,350	€90,650	€24,500	€220,500	€24,500
May, 2025	€268,571	€53,714.29	€61,771	€99,371	€26,857	€241,714	€26,857
June, 2025	€292,143	€58,428.57	€67,193	€108,093	€29,214	€262,929	€29,214
July, 2025	€315,714	€63,142.86	€72,614	€116,814	€31,571	€284,143	€31,571
August, 2025	€339,286	€67,857.14	€78,036	€125,536	€33,929	€305,357	€33,929
September, 2025	€362,857	€72,571.43	€83,457	€134,257	€36,286	€326,571	€36,286
October, 2025	€386,429	€77,285.71	€88,879	€142,979	€38,643	€347,786	€38,643
November, 2025	€410,000	€82,000.00	€94,300	€151,700	€41,000	€369,000	€41,000
December, 2025	€433,571	€86,714.29	€99,721	€160,421	€43,357	€390,214	€43,357
January, 2026	€457,143	€91,428.57	€105,143	€169,143	€45,714	€411,429	€45,714
February, 2026	€480,714	€96,142.86	€110,564	€177,864	€48,071	€432,643	€48,071

March, 2026	€504,286	€100,857.14	€115,986	€186,586	€50,429	€453,857	€50,429
April, 2026	€527,857	€105,571.43	€121,407	€195,307	€52,786	€475,071	€52,786
May, 2026	€551,429	€110,285.71	€126,829	€204,029	€55,143	€496,286	€55,143
June, 2026	€575,000	€115,000.00	€132,250	€212,750	€57,500	€517,500	€57,500
July, 2026	€598,571	€119,714.29	€137,671	€221,471	€59,857	€538,714	€59,857
August, 2026	€622,143	€124,428.57	€143,093	€230,193	€62,214	€559,929	€62,214
September, 2026	€645,714	€129,142.86	€148,514	€238,914	€64,571	€581,143	€64,571
October, 2026	€669,286	€133,857.14	€153,936	€247,636	€66,929	€602,357	€66,929
November, 2026	€692,857	€138,571.43	€159,357	€256,357	€69,286	€623,571	€69,286
December, 2026	€716,429	€143,285.71	€164,779	€265,079	€71,643	€644,786	€71,643

Risk evaluation and management

Risk No	Risk area	Risk Factor	Vulnerability	Threat	Likelihood (1-5)	Impact (1-5)	Total	Measures	Controls	Effectiveness of Controls
1	IT Department	Information Security	IT systems	Hardware failures	1	3	3	Double reservation of critical hardware units of every server Constant disk drive wearing monitoring and replacement before failure	reservation of critical hardware, software regular updates, disk drive ongoing monitoring	Strong
2	Corporate	Internal	Business operation	Entry into new markets (whether a new jurisdiction or product) in particular raise an increased risk in relation to market size, market share and demand. In addition to the change in consumer numbers, spend and competitors present, entry into new markets presents an additional risk of 'sunk' costs from investing	1	3	3	Sound business plan is drawn up and approved by the Board of Directors. Financing and support is fully obtained from the directors.	Licencing, business plan	Strong
3	AML department, IT team	Customer	Underage Players	Under Age customers attempting to gambling	2	2	4	Regular checks to verify DOB	Document verification controls	Strong
4	Financial Risk	Unforeseen Taxes and Regulations	Financial	The online gaming industry is still evolving, and tax regulations or gambling laws might change unexpectedly, impacting profitability.	2	2	4	Maintain Strong Legal Counsel and having a qualified legal team.	Actively monitor industry news and legal updates to stay abreast of developments that might impact your business.	Strong

Legal and governance framework

1. Overview of management structure

Managing Director, a corporate entity, is involved into both strategic oversight and day-to-day decision-making. This arrangement streamlines decision-making processes and enhances operational efficiency. The Ultimate Beneficial Owner (UBO) plays a pivotal role in setting strategic goals but does not involve themselves in the company's daily management activities.

2. Strategic Direction and Management

The Managing Director, empowered by the Articles of Association, is responsible for all operational decisions, ensuring that the company adheres to its strategic objectives while navigating day-to-day challenges. This centralized decision-making process allows for swift adjustments to market conditions and operational demands.

3. Reserved Matters and UBO Involvement

Key strategic decisions, such as significant financial investments, structural changes, and long-term strategic planning, require the input and approval of the UBO. While the UBO refrains from engaging in the company's day-to-day management, his involvement in these critical decisions ensures that the company aligns with their overarching vision and objectives.

4. Potential for Deadlock

Given the governance structure centered around the Managing Director, with strategic oversight from the UBO, the risk of deadlock is inherently low.

5. ESG Policy Consideration

Currently, the company does not have a formalized Environmental, Social, and Governance (ESG) policy.

Target KPI's and business objectives

Objective:

Establish Alisium BV as a profitable and reputable leader in the online gaming industry, with a focus on innovation, customer satisfaction, and sustainable growth.

Year 1: Foundation and Market Entry

- **Launch:** Roll out an engaging and diverse gaming portfolio. Secure partnerships with leading game developers to offer top-tier games.
- **Marketing:** Initiate a targeted digital marketing campaign focusing on key demographics in our launch markets. Utilize social media, influencer partnerships, and SEO to build brand awareness.

- Financial Target: Achieve a break-even point by Q4 through aggressive user acquisition and cost-effective marketing strategies.
- Customer Service Excellence: Establish a 24/7 customer support team dedicated to ensuring a seamless gaming experience. Measure success through customer feedback and aim for a 90% satisfaction rate.

Year 2: Growth and Profitability

- Revenue Goals: Target a 4-5% revenue growth quarter-over-quarter by expanding the game portfolio and enhancing user experience.
- Profitability: Implement cost optimization strategies across operations to reach a 10% profit margin by year-end.
- Player Base Expansion: Grow the player base by 15% through referral programs, loyalty rewards, and regular promotional events.
- Brand Building: Sponsor major gaming events and collaborate with well-known gaming personalities to solidify Alisium BV's market presence.

Year 3 and Beyond: Expansion

- Global Expansion: Enter 2 new markets each year, adapting our offerings to meet local preferences and regulatory requirements.
- Market Leadership: Leverage data analytics to refine user acquisition and retention strategies continually. Aim to secure a top 5 position in our target markets by year 5.

Key Performance Indicators (KPIs)

- Market Position: Track brand recognition and market share growth semi-annually.
- User Engagement: Analyze session lengths, and NPS scores quarterly.
- Innovation and Product Development: Technology upgrades annually.
- Regulatory: Conduct annual audits to ensure 100% compliance.

Execution Plan

- Q1-Q2, Year 1: Focus on platform development and initial user acquisition. Launch with at least 50 games.
- Q3, Year 1: Begin aggressive marketing campaigns and promotional offers to boost brand visibility.
- Q4, Year 1 to Q2, Year 2: Optimize operations based on user feedback. Aim for break-even by end of Q4.
- Year 2: Scale up marketing efforts based on analytics. Introducing loyalty programs. Begin planning for global expansion.
- Year 3: Enter new markets, continue to innovate with new game providers, and enhance user experience.

Policies and Procedures As the Project is still a startup below are the drafts of Policies.

Alisium B.V.

**Anti-Money Laundering and Counter Terrorism Financing Policy and
Procedures**

Table of Contents

1.	Version Control.....	2
2.	Terms and Abbreviations.....	4
3.	Company Policy.....	5
4.	Objective of the Policy.....	5
5.	Regulatory Framework.....	7
6.	Role of Compliance.....	7
7.	Definition of money laundering.....	8
8.	What is Terrorism Financing?.....	9
9.	Player Acceptance Policy.....	10
10.	Risk Management and Risk-based Approach.....	10
11.	Customer Due Diligence.....	12
12.	CDD and On-Going Monitoring Process Record Keeping.....	15
13.	Correspondence with the Client.....	15
14.	Document Translation and Certification.....	15
15.	Acceptable Identity Verification Documents.....	16
16.	Acceptable address confirmation documents.....	16
17.	Enhanced Due Diligence.....	16
18.	EDD during the course of business relationship.....	17
19.	On-going monitoring.....	18
20.	Periodic review.....	20
21.	Virtual Financial Assets.....	21
22.	Politically Exposed Persons.....	21
23.	Sanctions.....	22
24.	Dealing with sanctioned persons.....	23
25.	Termination of the business relationship.....	24
26.	Money Laundering Reporting Officer.....	25
27.	Reporting Requirements.....	26
28.	Reporting Procedure: Internal reporting.....	28
29.	Reporting Procedure: External reporting.....	28
30.	Dealing with the requests from the Authorities.....	29
31.	Tipping Off.....	29
32.	Training.....	30
33.	Staff recruitment.....	31
34.	Staff Responsibilities.....	32
35.	Record Keeping.....	32
36.	Funds Management procedure and Pay-out of gambling winnings.....	33
37.	Fictitious, Anonymous & Multiple Accounts (fraud management).....	34
38.	Business Risk Assessment.....	35
39.	Internal Controls and Compliance.....	35
40.	Verification of Partners	36
41.	Policy Revision.....	37
42.	Annex 1: Indicators of Suspicious Activity of Money Laundering / Terrorist Financing.....	38
43.	Annex 2: Examples of documents, that can prove client's source of funds/wealth.....	42
44.	Annex 4: KYC questionnaire for natural persons.....	44
45.	Annex 5: List of links to public registers.....	45
46.	Annex 6: Internal Suspicious Transaction Report.....	46
47.	Annex 7: Form to be completed by the MLRO upon receiving the above report from an Employee.....	47
48.	Annex 8: Partner form.....	48

1. Version Control

Name	Description
Document Name	Anti-Money Laundering and Counter Terrorism Financing Policy and Procedures
Version	1.0
Author	Compliance Department, MLRO
Authorised By	The Board of Directors
Distribution Date	
Review Date	

Version	Description	Date	Initials
1.0	Policy	03.2024	

2. Terms and Abbreviations

AML – Anti-Money Laundering

CDD – Customer Due Diligence

EDD – Enhanced Due Diligence

CFT – Combating the Financing of Terrorism

EDD – Enhanced Due Diligence

FIU – Financial Intelligence Unit (Curacao)

KYC – Know Your Client

ML/FT – Money Laundering / Funding of Terrorism

MLRO – Money Laundering Reporting Officer

PEP – Politically Exposed Person

NORUT – National Ordinance Reporting Unusual Transactions

NOIS - National Ordinance Identification when Rendering Services

STR – Suspicious Transaction Report

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.).

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 Customer 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 Terrorist Financing 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;

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

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist 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, to prevent the use of the financial system for the purpose of money laundering and terrorist financing.

The Company is incorporated in Curacao and is licensed and regulated by Antillephone N.V. to offer remote games over the internet, under the license conditions issued by Curaçao. The Company is required to have in

place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

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 (including but not limited to the Prevention and Suppression of Money Laundering and Terrorist Financing Law) 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 and terrorism financing. This AML/CFT 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 and combat the financing of terrorism 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 and the financing of terrorism. 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 terrorist 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 legislation.

5. Regulatory Framework

National regulations

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

- a) The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);
- b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c) The National Ordinance on Identification when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d) The National Decree contains general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
- e) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93);

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

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 or other criminal activities.

International regulations

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

On an international level, the FATF plays a very important role in the combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 39 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

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 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 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 risks;
- 4) Ensure sufficient resources for AML/CFT compliance and promote their efficient and expidient 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 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 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, but 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 MLRO 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 comparing 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 MLRO. 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 / behavior of the clients related to the 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 / behavior 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 MLRO 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 providing financial support to 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. Player 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 requirements;
- 5) It is known that the Client is or has been involved in Money Laundering or Sanctions breaches stories
- 6) The Client is resident of a restricted country
- 7) The Client is a Sanctioned Individual
- 8) Suspicious Transaction Report has been filed to FIU and / or 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 risk

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.

10. Risk Management and Risk-based Approach

Client ML/FT 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 main place of business or where the activity generating the Client's wealth is carried out.

Client risk Client risk is the risk of ML/FT 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 the beneficial owner.

The product, service or transaction risk is the risk one 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.

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/TF 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

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 ANG 3000 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 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 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, System reports on big deposits, 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

11. Customer Due Diligence

1. The Know Your Client (KYC) process, as part and parcel of the Company's ML/FT 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. General Terms and Conditions of the Company provides for the due diligence process that must be carried out before the opening of a Client account.

3. 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
- 8) Statement regarding PEP status

4. If a Client is a PEP / Family member of a PEP or Close Associate of a PEP, the match is reported to the MLRO. The Employee shall act in accordance with the Section 22.

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. At this point the Client is asked to provide identity verification document, which is reviewed by the Employee and screening against PEPs/Sanctions lists is performed and results are reviewed by the Employee. If screening results in matches, the Employee shall analyze matches and act as described further in this Section.

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

7. Upon any payment of ANG 3000 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 a selfie with the ID document and proof of address in addition to the previously obtained Client's identity verification document;
- 3) Screening of the Client against PEPs / Sanctions / Adverse Media lists
- 4) Client risk assessment (Employee shall complete a Client risk assessment form as set out in Section 10 Risk management)
- 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 from Clients whose risk is higher than low by means of 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 continue using the services of the Company, *except withdrawal services*.

10. The Client is prohibited to withdraw any funds from his account until the Employee receives all the requested information in terms of CDD 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 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, perform Client screening against Sanctions and PEP lists, check availability of adverse media in public and reliable sources by using search engines, such as Google or Yandex.

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.pdf

19. If suspicions about the quality of the identity document occur, the Employee shall immediately contact the MLRO and act further in accordance with his instructions. The MLRO 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 MLRO 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 10 (Risk Management).

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 MLRO and the business relationship with the Client shall be terminated following the instruction of the MLRO. If the match is a false positive, the Employee shall proceed with the Client risk assessment;

2) If there is a true match with PEP individual, the match shall be reported to the MLRO along with the Client's details and relevant information obtained, and the Employee shall await further instructions from the MLRO. 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 or other illegal activities, the Employee shall report the same to the MLRO by filing internal STR. The business relationship with the Client shall be suspended and the Employee shall await further instructions from the MLRO. If suspicions are grounded the MLRO 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 withdrawal restrictions are canceled at this point).

28. If the Client is assigned medium risk level, he shall be asked to complete KYC questionnaire. 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 risk increasing factors, the Client can proceed to use his account in a usual manner (the withdrawal restrictions are canceled at this point).

29. If the Client is assigned a high risk level, he shall be asked to complete the KYC questionnaire and the Employee shall escalate the case to MLRO by email. The employee shall provide the MLRO with the Client Profile

and await further instructions. The MLRO 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 MLRO and the business relationship with the Client should be terminated following the instructions of the MLRO.

31. The Company can continue to cooperate only with those Clients, who have fully complied with all CDD 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 and in the Client profile.

33. If the Client does not provide required information / documents or if the Employee is not satisfied that the purpose and nature of the business relationship are legitimate, the Employee shall:

1. Consider terminating the business relationship with the Client;
2. Consider the need to file an internal suspicious transaction report to the MLRO;

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

34. ***In case there is a need to file the internal suspicious transaction report, the MLRO 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 a suspicious transaction report should be filed.

35. If the business relationship with the Client is terminated, the MLRO 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, withdrawal restriction shall be canceled.

38. ***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 the CDD 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 CDD procedure.***

12. 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, as described below, in the Client Profile in the System.
2. The Employee shall verify all of the obtained information to the extent possible against publicly available reliable sources of information.
3. All 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.

13. 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.

14. 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 most employees and which can be easily translated into English, when necessary. Document translation must be certified as a true translation of the original.

15. 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

16. 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.

17. Enhanced Due Diligence

1. The Company must apply EDD measures in those situations that, by their nature, represent a higher risk of ML/FT. 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.
2. If the case occurs, where EDD must be conducted, the Employee shall inform the MLRO accordingly by e-mail and submit the Client Profile. The MLRO 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 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:
 - Unusually large transaction (over ANG 5000 or equivalent amount in other currencies) / transaction patterns made by the Client
 - There are questions on the funding method being used by the Client
 - 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;

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;
- 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;
- Other measures as may be indicated by the MLRO;

18. 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 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, 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 and Sanctions or other crimes;
- 9) Other factors that could pose the Company to higher ML/FT 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 analyzing 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 MLRO via the e-mail. The risk category of the Client should be indicated in the report. The MLRO 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 STR and act as set out in the Reporting procedure.

19. 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 11 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 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 and other type of fraud ***before 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
- 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
- Other relevant information.

The following automated tools are used for transaction monitoring:

- The System red flags the Clients, who request withdrawal without sufficient gaming activity.
- The employees receive daily reports on all transactions above 3000 ANG along with all the details of the users making those transactions.

In addition, an AI which is overseen by the MRLO will look for any unusual behaviour and report it right away to an Employee of the Company.

1. According to a risk-based approach and general experience the human employees will recheck all checks which are done before by the AI or other employees and may redo or do additional checks according to the situation. In addition, a data Scientist supported by modern, electronic, analytic systems will look for unusual behavior like:
2. Depositing and withdrawing without longer Betting sessions.
3. Attempts to use a different Bank account for Deposit and Withdraw, nationality changes, currency changes, behavior and activity changes as well as checks, if an account is used by its original owner.

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 MLRO 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 services provider has transaction monitoring systems in place which will allow for screening of the transactions pursuant to these provisions and in accordance with the applicable legislation. The MLRO shall be responsible to review the relevant service agreement with the service provider to ensure the adequacy of the agreement.

MLRO shall submit necessary reports to Antillephone and to the board of management of the Company as described further in the Antillephone Reporting Procedure (Appendix 9).

20. 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 than 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 MLRO.
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 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, 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.

21. Virtual Financial Assets

The Company considers Virtual Financial Assets (VFA) as being a payment method posing higher risk, than traditional payment methods. The Company shall abide the latest FATF issued recommendations and consider the latest identified risks related to the use of the Virtual Financial Assets when dealing with the clients, who use VFA as a payment method.

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

- 1) The threshold triggering CDD procedure shall be ANG 400 of total deposits.
- 2) Besides other measures, the control over the wallet shall be established in terms of the CDD procedure.
- 3) Any withdrawals shall be made to the same wallet, which has been used for placing deposits.
- 4) Transactions shall be monitored in the same way as for fiat currencies. However, additionally list of indicators of suspicious activity relating to the use of virtual financial assets was developed and is included in Annex 1. When dealing with the player who uses virtual financial assets 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 virtual financial assets.
- 5) 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 or TF, 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.
- 6) Transaction limits are usually set by the partner payment providers, however, standard limits are set by the Company and are: min 10 USD; max 10 000 USD.

22. 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 months, 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) 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. They are also asked to provide information on whether they are PEPs, Family members of a PEP, Known Close Associates of PEPs.
 4. 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 verified during business relationships with the client before processing any withdrawal request.
 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 MLRO 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 MLRO along with the customer's details and relevant information obtained, and the Employee shall await further instructions from the MLRO. The MLRO 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 MLRO shall be applied;
 - 3) Increased transaction monitoring shall be applied;
 - 4) The business relationship with such a customer is subject to the approval of the MLRO and Senior Management.

23. 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/>

All the potential customers of the Company are screened against current Sanctions lists prior to commencement of business relationship. The screening is also performed during business relationship with the client before processing any withdrawal request.

24. 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 report to the MLRO;
- Suspend the account of the Client until further instructions from the MLRO.

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

The MLRO 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 MLRO 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 the reliable information about Client's involvement in Sanctions breaches.

25. 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 MLRO will be notified so that it may be determined whether a report is to be sent to the relevant authorities.

2. 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. However, the risk of ML/TF should be considered before terminating the business relationship, taking into account all factors and information the Company has at its disposal about the Client.

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

- 1) Consider, if there is a potential ML/FT 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 MLRO.

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 suspicions.

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

If there are grounds to suspect ML/FT, the internal suspicious activity report has to be filed to the MLRO 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 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 STR to the MLRO and suspend the remittance pending the instructions of the MLRO.
- 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 in the remittance purpose.

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, Sanctions breaches.
- 2) The Client has been assigned unacceptably high ML/FT and Sanctions risk;
- 3) STR 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
- 6) The Client has been identified as attempting or participating in any criminal or unlawful activity

The Client's account shall not be closed unless the Company provides the Client with information that the closing is due to occur through a warning sent to the Client thirty (30) days before the account is due to become inactive.

26. Money Laundering Reporting Officer

Currently appointed MLRO: Maksims Rutenberg

Contact details:

e-mail: rutenbergsmaksims@gmail.com

Phone: +37122111700

Responsibilities of the MLRO

The MLRO core functions are:

1. To receive internal reports from the Company's employees, or through software solutions used; to further consider these reports and determine whether knowledge or suspicion of ML/FT subsists and to decide whether the report should be filed to FIU;
2. Where such knowledge or suspicion subsists, the MLRO must file the STR 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, or that a person may have been, is or may be connected with ML/FT;
4. To respond promptly to any request for information made by the FIU.

Other responsibilities of the MLRO:

- 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/CTF and Sanctions Regimes obligations.
- Development of the necessary AML /CTF, Sanctions Compliance policies, controls and procedures and maintaining those up-to-date and in line with any advice and/or guidance from the Financial Intelligence Unit, Antillephone and/or other relevant authorities;
- Addressing any FIU 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 /CTF policies, controls and procedures, as well as relevant up-to-date legislative requirements.
- Reporting to the board on a regular basis to highlight any changes in the AML/CTF and Sanctions Regimes Compliance framework.
- Submitting an Annual Report to the Board summing up the AML/CTF compliance within the Company
- Regular oversight reporting, including reporting of non-compliance, to the Board;
- Representing the Company to all external bodies and third parties in relation to AML/CTF and Sanctions Regimes Compliance;
- filing a report to FIU about each Company's refrainment from conducting suspicious transaction as soon as practicable.
- Maintaining a record of decision making as part of the reporting procedure
- Maintaining a register of disclosures and register of ML/TF 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/CTF Policy.

The MLRO 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 MLRO also provides the relevant authorities with the information about newly discovered ML / FT typologies and indicators.

27. 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.

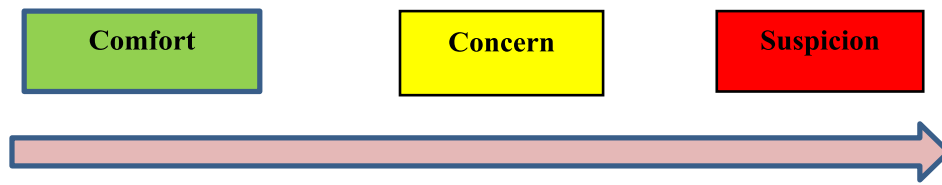
What constitutes knowledge?

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 MLRO
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 “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 MLRO.

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 suspicious transaction reports (STRs) 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 or terrorist financing;
3. **Consider** whether any Client's activity is unusual and potentially suspicious (see Annex 1 with the list of potential indicators of ML/TF)

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 STR).

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 STR).

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

28. 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, 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 suspicious transaction report to the MLRO.**

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 in respect of the client but there is no suitable indicator in the list provided, the employee **MUST** consider making the internal suspicious activity report to the MLRO and send it to the e-mail rutenbergmaksims@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 rutenbergmaksims@gmail.com with the e-mail subject "STR Submission".
2. Complete the form named "Internal Suspicious Transaction Report to the MLRO" from the 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 MLRO 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 MLRO.
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 MLRO 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 MLRO receives an internal suspicious activity report, he reviews it immediately, but not later than the next working day. The MLRO shall consider all the provided and other available information and shall decide whether the external suspicious activity report should be filed to FIU or not.
10. Where, following the consideration of an internal report the MLRO determines that no reporting to the Financial Intelligence Unit is required, the MLRO shall record the reasons for such determination in writing to the register of Internal Suspicious Activity Reports and, upon request, shall make it available to the Financial Intelligence Unit or other relevant supervisory.
11. The MLRO shall inform the Employee on further steps to be undertaken in relation to the Client.

29. Reporting Procedure: External reporting

As already described in the previous section, the MLRO shall receive and evaluate internal suspicion 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 or funding of terrorism, when such details are directly requested from the MLRO. This log shall be held by the MLRO and shall only be accessible to him, and will not form part of the Client's file. The MLRO 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 MLRO with relevant information.

1. Once the MLRO decides that there are reasonable grounds which warrant the submission of a STR the MLRO shall disclose that information, supported by the relevant identification and other documentation, to the FIU as soon as practicable, but not later than the next working day 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 MLRO will keep such records secure.
3. The MLRO 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 MLRO shall take such actions as required by the Authorities in connection with the disclosure and accordingly follow their instructions.

5. If the MLRO is of the view that there are no reasonable grounds for suspecting the activity to be related to ML/FT, but the MLRO believes that it would assist the Financial Intelligence Unit in the exercise of any of its functions, the MLRO may make a disclosure to the Financial Intelligence Unit.

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

Please refer to the Antillephone Manual for Reporting Procedure for further information related to the Company's reporting obligations.

30. Dealing with the requests from the Authorities

1. All the requests / inquiries from the Authorities must be deemed urgent.
2. The MLRO 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 MLRO via goAML portal, if not specified otherwise by the FIU.
5. The MLRO 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.

31. 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 a suspicious 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 STR 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 MLRO 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 MLRO

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 MLRO 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 MLRO 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 MLRO.

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 MLRO can provide guidance on such communications.

32. Training

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

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

- Employees have sufficient knowledge and awareness to detect money laundering / terrorism financing.
- 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.

Training plan shall be developed at the beginning of each financial period and approved by the MLRO 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:

- AML/CFT Policies 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 or the funding of terrorism.
- Record keeping obligations

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 Policy and relevant procedures.

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

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

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

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

The MLRO shall send periodic reminders of the need to report certain matters.

33. 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 all 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, MLRO 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 policies and procedures can be a sufficient reason for termination of employment.

34. Staff Responsibilities

All staff is required to:

1. At all times comply with the Company's AML Policies, Procedures and other internal control systems, including all measures relating to anti-money laundering and counter terrorist financing procedures;
2. Disclose any suspicion of money laundering and terrorist financing to the MLRO.

35. Record Keeping

The Company shall maintain appropriate records of all the Clients and their associated transactions for the purposes of ML/FT risk management and the prevention, detection, analysis and investigation of money laundering or funding of terrorism 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 or beneficial owner 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 suspicious transactions (Register of Internal Suspicious Transaction Reports), including a record of any written determinations made;
- 5) Register of any disclosures made to the FIU (Register of External Suspicious Transaction Reports)
- 6) Record 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 STRs 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 and the funding of terrorism 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.

After the elapse of the above-mentioned period, the documents related to the client identification, the data or information about the client must be disposed, unless the FIU or other relevant authority requires the Company to retain the above-mentioned documents for a longer period specified by them.

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.

36. 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 Client's 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 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 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 has equivalent AML/CFT 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. The transactions are analysed on the aspects of possible fraud / ML / FT, gaming activity before paying the funds out.

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

Again, 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 MLRO, that if the client uses multiple payment methods, in particular within 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 STR to the MLRO, 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 Sweden, 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 MLRO. The employee also needs to consider filing of STR, where necessary.

37. 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 suspicious activity report for consideration of MLRO.

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 users. 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 MLRO and the accounts are considered to be blocked.

38. 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 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 the Website offers, the Clients to whom services are offered, transactions performed by these Clients, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on 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 at least annually.

39. Internal Controls and Compliance

The Internal Controls are developed and Compliance procedures for monitoring and testing compliance with the AML/CFT 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 environment including developments in relation to new legislation
 - Progress on internal developments in relation to Company's policies, procedures and controls for AML/CFT.

The MLRO 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 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
- 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 policies and related procedures. The MLRO 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 MLRO shall regularly review relevant information sources, such as the results of the national and supranational ML/FT 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.

40. Verification of Partners

1. Internal control procedures have been designed to comply with the regulations. Internal controls take the form of manual controls implemented on a daily basis by the Company's Operations Team (and/or Payments Team) and computer/automated controls inherent within the gaming system software.
2. Before signing any Software license agreement the Company shall check conformity of every potential Partner to the following requirements:
 - 1) on any website owned or controlled by Partner:
 - a) website contains terms and conditions on use of the website, including terms of responsible game. Terms and conditions contain a list of restricted territories conforming to the list of the Company in force at the time of the check; procedure of KYC providing sufficient anti-money laundering measures, that are in conformity with European Union law in force at the time of the check.
 - b) website contains true information of the potential Partner.
 - c) website contains contact information (email, phone number), where to apply in case of player complaints.
 - d) website contains reference to the valid gaming license (in case of existence of a validation link - validity of the gaming license has been checked via validation link) and the reference conforms with the information provided by the Partner to the Company.
 - e) website contains reference and links only to regulated payment mechanisms (make a list of all payment mechanisms contained on the website at the time of the check);
 - f) website does not accept payments from land-based wagering agents and/or cash-based wager aggregators, website does not contain any reference to such options (in case of a negative answer – make a list of references not conforming to this requirement).
 - 2) check via accessible means on reputation of the potential Partner – review of references, player and/or business - partner opinions, feedback on potential customers available in internet sources most trusted and mostly used in industry at the time of the check (provide citations and source) – gives positive results.
 - 3) check via accessible and most recognized sources in industry (e.g. search engines, websites, etc.) on existence of any kind of promotion material (advertisement, banner, etc.) of the potential customer and/or its website(s) and conformity of detected promotion materials to the following criteria - promotion material in question prima facie seems legal (e.g. at first sight does not contain reference or item of any obviously unlicensed intellectual property, illegal promise and/or statement).
3. Before signing any White Label Agreement the Company shall perform the following procedure:
 1. undertake a risk assessment, and ensure that evidence of Customer's identity is obtained and retained as appropriate for all partners. Due to the nature of the online gaming business, the Company shall conduct an enhanced due diligence process for all of its prospective Partners.
 2. The Company shall obtain from the Partner full amount of KYC documentation and information, included but not limited to:
 - Certificate of Incorporation
 - Memorandum and Articles
 - Appointment of First Directors and Shareholders
 - Latest Registers of Directors and Shareholders
 - the ownership and control structure of the Legal Person, partnership, Foundation, trust or similar arrangement;

- Certificate of Good Standing (where applicable; or other document confirming the active standing of the legal entity)
 - Certificate of Incumbency (where applicable; or alternative document confirming currently appointed directors and shareholders)
 - Details, incl. identity verification documents of Ultimate Beneficial owners (UBO), shareholders and directors
 - gaming licenses
 - Every Partner shall have to fill out a due diligence form as provided in Annex 8 (Partner form).
3. Once all the information requested is obtained, the Company sends a confirmation email to the Partner on the email inserted by the Partner in the registration form.
4. In addition to the due diligence process performed at initial acceptance stage, the Partners shall be monitored on an on-going basis.

41. Policy Revision

The AML / CFT Policy and related procedures are subject to review, update and amendments by the MLRO, 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, business geographical changes, as well as other newly discovered risks. In any case, the AML / CFT Policy and related procedures are subject to review and/or at least annually. The Company shall ensure external independent review of its AML /CFT policies and procedures in urgent situations, such as essential changes in AML/CFT legislation.

42. 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 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 Laundering¹:

¹ <https://www.fatf-gafi.org/media/fatf/documents/reports/Vulnerabilities%20of%20Casinos%20and%20Gaming%20Sector.pdf>
Alisium B.V.
AML/CFT Policy and Procedure

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

43. 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.
--	--

44. 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 Person²
- ☐ A Family Member of Politically Exposed Person³
- ☐ A close Associate of Politically Exposed Person⁴

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:

² "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)

³ 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

⁴ 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

Alisium B.V.

AML/CFT Policy and Procedure

45. 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.ytj.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

46. Annex 6: Internal Suspicious Transaction Report

Internal Suspicious Transaction Report

Specific to Employees to be submitted to the MLRO 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 firm's MLRO.

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 MLRO 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 MLRO 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 Money Laundering Reporting 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

47. Annex 7: Form to be completed by the MLRO upon receiving the above report from an Employee

Date received

Consideration of Disclosure:

Action Plan:

Outcome of Consideration of Disclosure:

Are there reasonable Grounds for suspicion?

Is consent required from the Financial Intelligence Unit (FIU) to any ongoing or imminent transactions which would otherwise be prohibited acts?

YES

NO

If YES, please record authorisation and “way forward” details received from the Financial Intelligence Analysis Unit

48. Annex 8: Partner form

Partner Form

In order to ensure our ongoing compliance with all Legal and Regulatory Requirements in relation to the prevention of Money Laundering and Terrorist Financing, we require you to provide the following information prior to the launch of Software.

Include additional sheets as necessary

Name of company, business address incl. country, phone number, e-mail address:	
Company MLRO-name, phone number, e-mail address:	
Company number and registered office:	
List of URLs or proposed URLs:	
License number and licensing authority	
List of Directors (name and country of residence)	
List of Ultimate Beneficial Owners who control 25 % or more of the business or businesses in the group (name and country of residence):	

☐ Please check this box to confirm that you will obtain and provide Company necessary AML documentation as required by Company.

☐ Please check this box to warrant that all information provided is complete and accurate.

Authorised signatory signature:

Printed name

Date

Information Security Policy

Policy No.: ISP - 001
Date of Issue: 21/02/2023
Audience:

Responsibilities	Name	Role	Company
Drawn up by:	Information Technology Department		Alisium B.V.
Revised by:			
Approved by:			Alisium B.V.

Log of Changes

Version	Editor	Date	Reason of change
1.1	IT Department	18/12/2023	Revision

1 Document Information

1.1 Introduction

Storage of any data on computers and transfer across the network eases use and expands our functionality. Commensurate with that expansion is the need for the appropriate security measures.

The Information Security Policy recognizes that not all business functions within the Company are the same and that data are used differently by various units.

The Policy is written to incorporate current technological advances. Instances of non-compliance must be reviewed and followed up by the Information Security Manager.

1.2 For use by

This Information Security Policy should be disseminated to all users including vendors, contractors, and business partners. This information security policy should be reviewed and updated at least yearly. All employees must sign an agreement verifying they have read and understood this document.

1.3 Permeable

Should positions within the Company, referred to within policies and procedures, be

vacant, the responsible Key Person is vested with all the applicable responsibilities. The Responsible Key Person is authorised to engage consultants and experts in meeting his responsibilities relating to technical, legal and similar issues.

2 Purpose, Objective and Scope

By information security we mean protection of the Company's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

The purpose and objective of this Information Security Policy is to protect the Company's information assets, including data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation, from all threats, whether internal or external, deliberate or accidental, to ensure business continuity, minimise business damage.

The purpose of the information security policy is:

- a. To establish an operation-wide approach to information security.
- b. To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of data, applications, networks and computer systems.
- c. To define mechanisms that protect the reputation of the Company and allow the same to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to worldwide networks.
- d. To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy.

3 Responsibility

The Information Security Manager is responsible for the regular updating, review, approval, publishing and implementation of the Information Security policy, management of information security and to provide advice and guidance on information security.

The Information Security Manager must ascertain that appropriate training is provided to data owners, data custodians, network and system administrators, and users.

Managers / Directors are directly responsible for implementing the Information Security Policy within their business areas.

4 General Policy

The Company adopts a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the operation's data, network and system resources. Vulnerability and risk assessment tests of external network connections are conducted on a regular basis.

5 Policies

Information must be protected from a loss of confidentiality, integrity and availability.

Regulatory and legislative requirements must be met.

Business continuity plans must be produced, maintained and regularly tested.

Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Education and training must be provided to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This must be tailored to the role of the individual network administrator, system administrator, data custodian, and users.

All breaches of information security, actual or suspected, must be reported to, and investigated by, the Information Security Manager. The appropriate Incident Reporting procedures must be followed.

Other guidance and procedures (such as system access control and backup procedures) within the company procedures manual support this policy. It is the responsibility of each employee to adhere to the Information Security Policy.

All employees have a responsibility to conduct themselves in an ethical manner.

Non-compliance with this Policy will be subject to Management review and action in conformance with the Company's disciplinary procedures.

5.1 *Data Classification Policy*

It is essential that all data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. Three classes of data have been identified:

5.1.1 High Risk

Information assets over which there are legal requirements for preventing disclosure. Data covered by local and international legislation, are in this class. Payroll, personnel, gaming, player and financial information are also in this class because of privacy requirements. This policy recognizes that other data may need to be treated as high risk because it would cause severe damage to the Company if

disclosed or modified. The data owner should make this determination. Access to High Risk data must be controlled from creation to destruction, and will be granted only to those persons who require such access in order to perform their job ("need-to-know"). Access to High Risk data must be individually requested and then authorized by the Data Owner who is responsible for the data. In addition, the dissemination of such information with third parties is prohibited from doing so without the express confirmation in writing by a member of the Executive Team and preferably the right of the third party to receive such information should be prescribed in a contract.

5.1.2 Confidential

Data that would not expose the Company to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. Access to such data shall be by default given solely to employees who maintain a managerial role within the company. Access to other employees may be given on a 'need to know' basis. The dissemination of such information requires the express confirmation by a member of the Executive Team.

5.1.3 Public

Information that may be freely disseminated. Access to such information need not be controlled although specific guidelines may be issued by the Executive Team if they perceive the dissemination such information to be harmful to the business.

No system or network subnet can have a connection to the Internet without the means to protect the information on those systems reflecting its confidentiality classification.

Data custodians are responsible for creating data repositories and data transfers which protect data in the manner appropriate to its classification.

High risk data and confidential data must be encrypted during transmission over insecure channels.

All appropriate data should be backed up, and the backups tested periodically, as part of a documented, regular process.

Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks destroyed consistent with industry best practices for the security level of the data.

5.2 *Access Control / Password Policy*

Data must have sufficient granularity to allow the appropriate authorized access.

There needs to be a balance between protecting the data and permitting access to those who need to use the data for authorized purposes.

Access to the network and servers and systems should be achieved by individual and unique logins and should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.

All systems which store sensitive information such as passwords must do so using non-reversible encryption.

Users must not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. Exceptions may be allowed under specific scenarios and under specific authorisation by the Information Security Manager. All users must secure their username or account, password, and system access from unauthorized use.

Users are accountable for the security and use of their user accounts and passwords.

System user accounts should regularly be reviewed and audited for malicious, obsolete, and unneeded accounts. Inactive accounts should be disabled.

Passwords associated with Logon IDs must comply with the Password policy of the Company. All users must have a strong password. Basics for creating a strong password include minimum length being of eight characters which should include a mix of uppercase, lowercase, and numerical characters. Empowered accounts, such as administrator, must be at least eight characters long, contain at least one numerical and one special character, and be regularly changed.

Any sensitive system supporting the infrastructure or that would allow indirect access to data should be protected with multifactor authentication such as Google Authenticator to prevent access of such systems even if usernames and passwords are leaked. The infrastructure should additionally be restricted to be able to be accessed only by certain physical computers and via a private VPN.

Should a user of any system forget his or her password, the password will be reset by the systems administrator. The system must prompt the users to enter a new password immediately upon the first login attempt.

All system passwords must be changed every 60 days for security purposes. Encrypted passwords should be enabled on any devices where it is not on by default. Back-end systems should have an automatic inactivity log-off period of 1 hour.

Users who leave their workstations must lock their workstation or log off to prevent

unauthorized access. Users which fail to comply with this policy will be held liable for the use of their account and disciplinary action may be taken.

Default passwords on all systems must be changed after installation.

Terminated employees should have their accounts disabled.

Monitoring must be implemented on all systems including recording logon attempts and failures, successful logons and date and time of logon and logoff.

Accounts should be locked automatically after multiple password failures in any system which supports such functionality. If a system does not support such a feature, the Information Security Manager should regularly review the access logs of that system, to ensure that user accounts are not being mismanaged.

Activities performed as administrator or super user must be logged by the system and where the system does not allow such logging, compensating controls put in place.

Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.

System logs should be reviewed regularly.

5.3 Virus Prevention Policy

The introduction of computer viruses into the Company's environment is prohibited, and violators may be subject to prosecution.

Desktop and laptop computer users shall not write, compile, copy, knowingly propagate, execute, or attempt to introduce any code designed to self-replicate, damage, or otherwise hinder the performance of any computer system (e.g. virus, bacteria, worm, Trojan horse, or the like).

Headers of all incoming data including electronic mail must be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned.

System or network administrators should inform users when a virus has been detected.

Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

Users must not tamper with or disable anti-virus software installed on their workstations.

Users must do their best to contain any spread of malicious software within the company's environment.

Suspected viruses should be reported immediately to the Information Security Officer. Alisium B.V. shall immediately inform the relevant authorities as soon as malicious code or suspicious codes are discovered in the system. Alisium B.V. shall also take the necessary immediate steps to ensure that the malicious code does not affect the Alisium B.V.'s systems and Alisium B.V. Information stored therein.

5.4 Internet Security Policy

All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified high risk and/or confidential.

5.5 Email Policy

Email equipment is outsourced.

Messages that are created, sent or received using the Company's denoted email system are the property of the Company.

The Company reserves the right to access and disclose to relevant entities the contents of all messages created, sent or received using its email system.

Users must be very careful when opening email attachments.

All email communication must be handled in the same manner as a letter, fax, memo or other business communication.

Sensitive data in the email or any attachments must not be transmitted in clear text over the Internet.

Any urgent Virus warnings should be channeled to the Information Security Manager for verification of authenticity.

Email messages should not have any content that may be considered offensive or disruptive. Offensive content includes but is not limited to obscene or harassing language or images, racial, ethnic and sexual or gender specific comments or images or other comments or images that would offend someone on the basis of their religious or political beliefs, sexual orientation, national origin or age.

Employees may not retrieve or read email that was not sent to them unless specifically authorised by the Responsible Key Person or by the email recipient.

Employees may not execute attachments to emails received when these are executable files.

Company email may not be used for personal reasons.

5.6 *Portable Computer and Media Policy*

Personnel computers, laptops and workstations issued by the organization are viewed as the company's assets and must be adequately protected.

Laptops, and their peripherals are popular targets for thieves. Since these assets are highly vulnerable to unauthorized access or theft, they present unique risks in the areas of disclosure, modification or destruction of proprietary information.

During the normal workday, whether working in an office or at an off-site location, employees are strongly encouraged to use a security cable to fasten the laptop to a desk, chair or other fixed object.

Employees should never leave a laptop on the desk, in the work area or in any other visible location overnight. Portable media should be locked in a secured area at the end of the workday.

When transporting a laptop or peripheral, employees should never leave it unattended in a visible location or in an unlocked vehicle.

When traveling with a laptop, never check it with other baggage.

In the event a laptop is stolen (regardless of where the theft occurs), employees should immediately file a police report and notify the Responsible Key Person immediately. A copy of the police report should be submitted to the Information Security Manager/ Management Team.

All assigned laptops, peripherals, related equipment and media remain the property of the company and are to be returned upon request, or when a staff member leaves.

All of the organisations' owned or leased facilities, equipment, related components and resources should be protected from unauthorized physical access, damage, loss from theft or other risks.

All media that becomes obsolete such as PCs, hard-drives, USB memories, CDs must be handed in to the Information Technology & Technical/ Management Team for proper disposal in accordance with the media disposal policy.

Adequate building security should be provided, and all facilities should be well-maintained, clean and free from safety or fire hazards.

Users must ensure that their portable PC is securely stored when not in use.

When outside of the office, employees should avoid leaving their PC unattended in their car. If it is inevitable to leave a PC in a car, it should be stored out of sight, e.g. in the boot.

PCs must never be left unattended while traveling on public transport.

5.7 System Security Policy

All systems connected to the Internet should have a vendor supported version of the operating system installed.

All systems connected to the Internet must be current with security patches.

System integrity checks of host and server systems housing high risk data should be performed.

All player activity shall be communicated over a secure communication protocol.

6 ACCEPTABLE USE & ETHICS

1. Any computer resources must be used in a manner that complies with the Company's policies.
2. The company will monitor the use of office systems.
3. All control system events are logged.
4. Unauthorised access to office systems is an offence.
5. It is against our policy to install or run software requiring a license on any computer without a valid license.
6. Use of the Company's computing and networking infrastructure by employees unrelated to their positions must be limited.
7. Use of the Company's computer resources for personal profit is not permitted.
8. Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations.
9. All data contained on, or passing through corporate assets is subject to monitoring and remains the property of the corporation.
10. Under no circumstances is an employee authorized to engage in any activity that is illegal under local or international law while utilizing company-owned resources.
11. Employees must not use company accounts to post publicly accessible messages or posts without permission.
12. Users are expressly forbidden to install any software on their workstations without prior approval from their supervisor.
13. Portable personal media should not be connected to company equipment and should not contain company documents.
14. Users may not perform vulnerability scans, monitor network traffic, or perform any action that is designed to escalate privileges or gain access to information that was not expressly intended for them.
15. Users must not reveal any information about company clients, employees, business practices, technology, schedules, or any other information not already publicly available to any outside resource or person without expressed permission from their supervisor.

16. Users must not use their company email accounts for purposes other than the conduct of company business. Forbidden actions include any and all forms of harassment, phishing, solicitation, spamming, forwarding chain letters and pyramid schemes, conducting personal business, and general personal correspondence.

6.1 Firewalls

Firewalls should be configured to "Deny" all traffic that is not explicitly "Allowed".

Firewalls should filter both inbound and outbound (ingress and egress) connections, limiting them to that which is required to conduct business.

6.2 Servers and Workstations

Databases will only store entire credit card details if the company acquires a PCI compliance certificate. The company currently encrypts all credit card details stored in the database.

Publicly accessible web servers should be located on a network which is both logically separated and secured from the internal systems network.

Mobile computers that connect to the internet must have a personal firewall and up-to-date anti-virus software installed.

Antivirus scanners should be installed on all servers and workstations and should be updated with the latest virus definitions.

All development, testing, and production systems should be updated with the latest vendor security patches.

6.3 Assets Deployment and Maintenance

All changes to firewalls must be reviewed and authorized by the Information Security Manager and logged for future reference. Changes to the production environment should be authorized and logged before being implemented.

When an employee leaves the company, that employee's company user accounts and passwords should be immediately revoked.

Remote maintenance accounts should be enabled when needed and disabled when the maintenance process is completed.

Access to sensitive data should be logged where practically possible.

Successful and unsuccessful login attempts and the accessing of the audit logs should be logged.

System clocks should be synchronized, and log files should contain date and time stamps.

The firewall, router, and wireless access point logs should be regularly reviewed for unauthorized traffic.

Audit logs should be regularly backed up, secured, and retained for at least three months online and one year offline for all critical systems.

Wireless analyzers should be periodically run to identify all wireless devices.

Vulnerability scans or penetration tests should be performed on all applications and systems before they are put into a production environment. Before going into production, all devices must undergo a lockdown procedure where unnecessary or default services, protocols, settings, accounts, and passwords are changed or disabled.

Only secure, encrypted communications should be used for remote administration of production devices.

6.4 *Physical Security and Access Control*

Multiple physical security controls should be implemented to prevent unauthorized access to data centers.

Equipment and media containing sensitive information should be physically protected from unauthorized access.

The distribution and disposal of backups and other media containing sensitive information should be in accordance with a procedure approved by the Information Security Manager.

Media that contains sensitive information should be inventoried and securely stored.

Media that contains sensitive information should be deleted, shredded, or degaussed before disposal.

6.5 *Wireless Communications*

All wireless access points must be configured with encryption, MAC filters, or technology that limits access to those devices that are explicitly authorized.

Networks with wireless access should be separated by a firewall from networks that handle sensitive information.

Wireless access points that support WPA2 should be configured to use it.
Wireless communications should be encrypted with WPA2, or 128-bit SSL.

6.6 *Clean Desk and Clear Screen Policy*

Clear desk and clear screen policy used to reduce the risks of unauthorized access to, or loss of, or damage to, information.

Ensure that appropriate facilities are available in the office in which, depending on their security classification, computer media (disks, tapes, CDs) and paper and paper files can be stored and locked away, including in lockable pedestals, filing cabinets and cupboards.

Personal computers should be locked when not in use and should be password protected.

Everyone should be required to use a password protected screen saver that automatically fires up after only a few minutes of inactivity.

Incoming and outgoing mail collection points should be protected or supervised so that letters cannot be stolen or lost, and faxes and telexes should be protected when not in use.

All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

7 Security in Supplier Relationships Policy

7.1 *Purpose*

The purpose of this policy is to ensure proper protection of the Company's assets that are accessed by suppliers.

7.2 *Scope*

This Security in Supplier Relations Policy applies to all business processes and data, information systems and components, personnel, and physical areas of the Company.

7.3 *Policy*

Information Security in Supplier Relationships:

- Procedures surrounding risk mitigation of a supplier's access to [the Company's assets must be documented, reviewed, and agreed upon by the Company and the specific supplier.
- All suppliers that access, process, store, or provide various IT components must be in agreement with the Company's security requirements around suppliers' relationship with the assets.
- Types of information access should be defined that different types of suppliers will be allowed, as well as monitoring and controlling the access
- Types of obligations applicable to suppliers should be defined to protect the organization's information.
- Security requirements agreements for suppliers must also include details on addressing risks surrounding the handling, processing, and communicating of assets or services.
- Processing facilities from business processes involving external parties shall be identified and appropriate controls implemented before granting access.
- Legal and regulatory requirements, including data protection, intellectual property rights, and copyright, etc. should be clear identified and addressed.

7.4 Supplier Service Delivery Management:

- A process must be developed to monitor and assess the service delivery of a supplier to ensure it is meeting appropriate business and security requirements, as well as meeting any contract or SLA requirements.
- A change management process must be in place to address any alterations to an existing policy, including documentation of said change and ensuring it is in alignment with business processes and follows appropriate re-assessment of risk involved, if necessary.

8 Third Party Access Policy

Third parties occasionally conduct business/provide services to the Company and thus require network communication. Access is only given to third parties after request is received from one of the company Executives who must also specify the level of access required by such person which must be assigned by the Chief Technology Officer.

The following guidelines apply in giving access to third parties:

- The third party must be covered by a contractual undertaking which binds the third party to security measures which are equivalent to the measures specified within the security policies of the company. Where no such contractual undertaking is present, the third party must sign a declaration confirming acceptance of the security policies of the company.
- Access to third parties must respect data protection laws. The third party shall only be

given access to the databases of the company where it is absolutely necessary for the third party to have access to them given the nature of the work and service the third party must provide to the company.

- Where a third party requires a remote connection to the company's network the remote access policy shall be read in conjunction with this policy. The third party's access shall be closely monitored and removed immediately when the purpose for which it was given has been exhausted.
- All third party network connections will be reviewed on a yearly basis and information regarding specific third party network connections will be updated as necessary. Obsolete third party network connections will be terminated immediately.
- Third party access to contracted service providers must be terminated as and when software contracts are terminated/expired.

8.1 Document, Equipment and Media Disposal

The company hardware and media is co-located on the premises of Data Centres (DC) in Europe and in Curacao . This document explains the company's procedure to make sure that information is not made available to unauthorized personnel in case any equipment / media is to be removed from the premises mentioned above or in case that a piece of equipment is to be made entirely redundant.

Equipment / Media containing confidential data must be marked "Confidential" to indicate this without requiring it to be read.

8.2 Faulty Equipment / media located at the ISP

If any equipment / media is faulty it will have to be replaced, the DC will be providing such equipment. Changes will be carried out by authorized personnel at the DC and if need arises by an appointed third party authorized personnel. Personnel authorization forms will be provided and kept up to date with the DC to ensure that only authorized persons can enter the data center and work on the company's servers. In case of faulty hardware / media and emergency action required the Responsible Key Person and the appointed third party authorized personnel shall have 24 hour access to the data center. If any equipment needs to be removed from the data center then the approval of the Responsible Key Person must be sought and the appropriate information submitted to the GCB within 72 hours of decommissioning. Any equipment /media that is to be removed from the data center falls under the Responsible Key Person's care and custody.

Hardware / media that has been cleared for removal from the data center and for its subsequent disposal/recycling is to first be checked to ensure that it contains no data or information; it will then be safely stored in a locked cabinet under supervision of the Responsible Key Person. The Responsible Key Person will then be responsible for the full disposal/recycling. Hardware / media will be demagnetized / degaussed prior

to manual disposal / recycling. Any failing hard drives will be immediately exchanged for new hard drives. Failing hardware / media that does not contain any data will be destroyed and disposed of / recycled. If any equipment is to be installed to replace the faulty equipment the installation will be completed to allow the operation to continue. The GCB will then be informed and called in to seal the new equipment and the GCB Equipment Form will be completed.

8.3 *Redundant Equipment / media located at the DC*

In case of any equipment at the data center that is to be made redundant the RESPONSIBLE KEY PERSON will inform the GCB through the submission of an incident report and also fill in and submit the Decommissioning Equipment Form for authorization from the GCB. Once approval is obtained the equipment is removed from the data center. The responsible key person will then be responsible for disposal / recycling of respective hardware. If any equipment is to be installed to replace the redundant equipment the GCB's approval will be sought prior to installation.

8.4 *Redundant Equipment/ Media located in the office*

The hardware / media will be safely stored in a locked cabinet under the supervision of the responsible key person. If it is to be disposed of it will be demagnetized / degaussed prior to disposal / recycling.

Company documents should be shredded prior to disposal.

An incident report with the full explanation and action taken will be submitted to the GCB within 24 hours of the occurrence of any incident. If the incident is a planned incident then the GCB will be given prior notice and authorization requested when necessary.

8.5 *Player Password and Payment Information*

All player passwords and payments must never be stored, received or passed in clear text.

This data will always be encrypted in line with this policy using MD5or SHA-1 algorithms.