

Anti-Money Laundering and Countering Financing of Terrorism Policy

Sunrise Worldwide Solution N.V.

Sunrise Worldwide Solution N.V

Document Information

Subject	Anti-Money Laundering and Countering Financing of Terrorism Policy
Purpose	XX Policy document containing policies to comply with ML Legislative and Regulatory requirements.
Involvement	All departments
Responsibility	Money Laundering Reporting Officer
Approval	Directors
Review	Annually or earlier as needed
Classification	Company Confidential

Change history

Date	Ver.	Author	Summary Changes	Director
	1.0	Anti-Financial Crime	New document created as part of AML/CFT Program review	

Contents

Contents.....	
DEFINITIONS:	5
ABBREVIATIONS:	8
1. Introduction	9
2. Scope	11
2.1. What is Money Laundering?	11
2.2 Anti-Money laundering policy within the Company	13
2.3 What is Terrorism Financing?	13
3. Proliferation Financing	16
3.1 Targeted Financial Sanctions	17
4. Anti-Money Laundering Compliance	17
5. The Role of the MLRO	18
6. The Risk Committee	19
7. Risk Assessment	20
8. Business Risk Assessment (BRA)	20
9. Customer Risk Assessment (CRA)	23
10. Client Screening	23
9.2 Negative Media	25
i) Financial Crime	26
iv) Fraud	26
11. Risk Factors specific to the Gambling Sector	27
Geographical risk	27
Product, Service and Transaction Risk	28
12. Risk Assessment - A dynamic approach	28
13. Customer Due Diligence	29
14. Onboarding of New and Prospective Clients	30
15. Client Categorisation Criteria	31
16. Measures relating to CDD- Procedural Controls	39
16.2 Carry out a customer risk assessment	40
16.3 Verification of identity	41
17. Obtaining information on the purpose of the business relationship	41
18. Ongoing and Transaction Monitoring	41
19. Timing of CDD Measures	43
20. Identification and verification of the Beneficial Owner	44

21.	Enhanced Due Diligence (EDD).....	44
22.	Mandatory Enhanced Due Diligence.....	44
23.	Simplified Due Diligence	45
	Simplified Due Diligence (SDD) is employed where the risk of money laundering is lower.	
	Measures include:.....	45
24.	Termination of the business relationship.....	46
25.	Reliance on third parties to perform CDD	46
26.	Payment Methods	47
27.	Notifications of Fraud, ML/FT, and Law Enforcement or Regulatory Authorities' requests 48	
28.	Reporting Obligations.....	48
29.	Suspicious Transaction Report	49
30.	Prohibition of Disclosure	49
31.	Record-keeping	49
32.	Employee training	49
33.	Employee screening.....	50
34.	Risk Appetite	50
35.	Customer Acceptance Policy	51
36.	Reporting to the FIU.....	53
37.	Thresholds Limits and Controls.....	54
38.	Jurisdiction Risk	55
39.	Policy, Compliance and Review	56
30.	Conclusion	57

DEFINITIONS:

“Money laundering” means:

- a) the conversion or transfer of property, knowing or suspecting that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.
- b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing or suspecting that such property is derived from criminal activity or from an act of participation in such an activity.
- c) the acquisition, possession, retention or use of property, knowing or suspecting, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity.
- d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counselling the commission of any of the actions referred to in points (a), (b) and (c).

“Senior management” means an officer or employee with sufficient knowledge of a company's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, who does not need, in all cases, to be a member of the board of directors.

“Terrorist financing” means the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, to carry out any of the offences within the meaning of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism.

“European Economic Area (EEA)” means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.

Sunrise Worldwide Solution N.V

“EU Directive” means the Directive 2015/849/, EU 847/2015, EC 1781/2006 of the European Parliament and the Council of May 2015 on the prevention of the use of the financial system for Money Laundering and Terrorist Financing.

“Money Laundering and Terrorist Financing” means the money laundering offences and terrorist financing offences defined in the Law.

“Manual” means the Policy on Know Your Customer (KYC) & Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) which has been drafted and adopted according to the EU Directive.

“Occasional Transaction” means any transaction other than a transaction carried out during an established Business Relationship formed by a person acting during financial or other business.

“Clients” means customers utilising Sunrise World Solution N.V. services

“Other Business Activities” includes the following trust services and company services to third parties:

- forming companies or other legal persons.
- acting as or arranging for another person to act as a director or secretary of a company, a partner of a partnership or a similar position in relation to other legal persons.
- providing a registered office, business address, correspondence or administrative address and other related services for a company, a partnership or any other legal person or arrangement.
- acting as or arranging for another person to act as a trustee of an express trust or a similar legal arrangement.
- acting as or arranging for another person to act as a nominee shareholder for another person.

“Politically exposed persons” means natural persons who are or have been entrusted with prominent public functions, other than middle ranking or more junior officials. The definition also covers their immediate family members or persons known to be close

associates of such persons.

For the purposes of this definition the term "natural persons who are or have been entrusted with prominent public functions" includes the following both local and foreign :

- Heads of State, Heads of Government, Ministers, Deputy or Assistant Ministers, and Parliamentary Secretaries.
- Members of Parliament or similar legislative bodies.
- Members of the governing bodies of political parties.
- Members of superior, supreme, and constitutional courts or of other high-level judicial bodies whose decisions 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 boards of State-owned enterprises.
- Anyone exercising a function equivalent to those set out in paragraphs (a) to (f) within an institution of the European Union or any other international body.
- Family members include the following:
 - the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
 - the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
 - the parents of a politically exposed person;
- Persons known to be close associates means:
 - natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
 - natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

"Business Relationships" in accordance with the definition provided in the PMLFTR business relationships must comprise three important cumulative elements, which are the following:

- the relationship must be of a business, professional or commercial nature between two or more persons;
- at least one of the persons involved in the relationship must be a subject person (whether undertaking a relevant financial business or a relevant activity); and
- the relationship has, or is expected to have at the time when the contact is established, an element of duration.

ABBREVIATIONS:

“AML” Anti-Money Laundering

“BRA” Business Risk Assessment

“CDD” Customer Due Diligence

“CRA” Customer Risk Assessment

“CTF” Counter-Terrorist Financing

“EDD” Enhanced Due Diligence

“FIU” Financial Intelligence Unit

“FS” Financial Sanction

“FT” Funding of Terrorism

“KYB” Know your Business

“KYC” Know Your Customer

“ML” Money Laundering

“MLRO” Money Laundering Reporting Officer

“SAR” Suspicious Activity Report

“SDD” Simplified Due Diligence

“STR” Suspicious Transaction Report

1. Introduction

“Money laundering” (ML) is generally defined as “engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally derived proceeds so that those proceeds appear to have been derived from legitimate activities or origins or otherwise constitute legitimate assets.” Further discussion shall be had in the next section.

The “proceeds of crime” are funds derived from illicit sources and from which a benefit or enjoyment may be obtained. Although the aim may not be to launder the funds or to fund terrorism it is still considered to be an illegal activity and subject persons should be aware of such activity and must report it as if it was ML or Financing of Terrorism (FT).

The policies set forth herein (the “Policies”) are intended to satisfy the statutory requirements of the relevant legislation and to provide direction to XXX (the “Company”) in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism. Based on the requirements of various statutory obligations, including the National Ordinance when rendering services, the National Ordinance on reporting of unusual transactions, the Sanctions National Ordinance, and the Kingdom Sanctions Act, and the Regulations for Combating Money Laundering, Financing of Terrorism, and the Proliferation of Weapons of Mass Destruction, and other pertinent legal instruments (collectively “Curacao AML/CFT laws”, please *vide* the Communication from the Curacao Gaming Control Board (Ref: GS/U215/24), pg 1 et seq), the Company has taken a position on who can and cannot be accepted as a customer.

The Company is aware that criminals and terrorists may attempt to use the Company’s services to channel funds from illegal activities.

The National Ordinance on the Reporting of Unusual Transactions (NORUT) provides indicators to help identify unusual transactions. These indicators (consisting of objective and subjective indicators) describe when an (executed or intended) transaction is to be labelled as unusual, and thus should be reported to the pertinent national authorities. The Curacao AML/CFT laws also provide statutory obligations which the Company shall adhere to as to indicators and regulations as to customer acceptance or otherwise.

Indicators are as follows:

Objective Indicator: In this case, the reporting entity is obliged to report an unusual transaction. The list of objective indicators describes under which circumstances a transaction is to be considered as unusual. Objective indicators may include the following:

- A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
- An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions

National Ordinance;

- A transaction giving cause to assume that it may be connected with money laundering or terrorist financing.

A transaction amounting to NAF 4000 or more, regardless whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner;

- A giro-based transaction amounting to NAF 4000 or more: A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank account carried out at the request of the client addressed to the service provider.
- The taking into deposit or the releasing out of deposit of an amount of NAF 4000 or more, at the request of the client.
- Sale of tokens to a client in the amount of NAF 4000 or more. The term "tokens" includes at least chips and credits.
- Payout of prizes in the amount of NAF 4000 or more.
- All other cases

Subjective Indicator: In case of a subjective indicator, the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, their gaming (-related) activity and any other circumstance that may be relevant) has reasonable knowledge to presume that a transaction is related to money laundering or terrorism financing. In case the answer to this assessment is yes, then the reporting entity has the obligation to report.

The Company has in place appropriate systems and controls to forestall ML and FT occurring through its business and/or its business being used for ML/FT. This policy contains the procedures that the Company has developed to comply with these obligations. This policy is to be read in tandem with the Company's internal controls and compliance management procedure.

The extant regulations require that an organisation has to have an individual having the requisite qualifications of a Money Laundering Reporting Officer (MLRO) to ensure that there is up-to-date knowledge of issues relating to Anti-Money Laundering and Countering of the Financing of Terrorism (AML/CFT) throughout the Company. The Policies and Procedures are hereby in place to provide knowledge and processes to prevent the company from being used for illicit activity and to receive reports of suspicious activity where necessary.

The Company serves as a remote gaming operator and shall only be offering the service of Casino holding a **0GL/2024/117/0107**. The Company shall adhere to the three lines of defence being customer support and client facing positions, the MLRO and the internal or external audit function.

Notice:

All employees will be required to read this manual and to confirm in writing that they understand their personal responsibilities arising from the policies and procedures which are set down here along with the Companies corporate responsibilities under the extant Curacao ML/FT laws, and pertinent AML/CFT legislation.

2. Scope

The scope of this policy is to establish policies and procedures on internal controls, risk assessment, risk management and compliance in relation to AML and CTF.

The policy has been created in compliance with the licence held within the Curacao jurisdiction and ensures to:

- Remain alert to the possibility of ML or FT;
- Report all suspicions to the MLRO email address in accordance with the AML/CTF policy and SAR procedures;
- Comply fully with all AML procedures including: Client identification, monitoring, record keeping, awareness and reporting in accordance with their respective roles and responsibilities within the company;
- Attend any relevant training and updates provided by the MLRO, keeping up to date with new and evolving threats;
- Complete the mandatory AML/CFT Training periodically to ensure compliance and adherence to the policy;
- Ensure that the company is not used for illicit activity;
- Take the most reasonable and appropriate actions to mitigate the risks associated with ML, FT, and other financial criminal activities, including fraud, corruption etc.
- This policy & procedure is applicable to all employees, contractors, affiliates and any other individual working on behalf of the company. The company is determined and committed to prevent the carrying out of financial activities through its systems that may be related to ML or FT.

The Company shall comply with its obligations at law by establishing the necessary and relevant processes to prevent ML and FT and to ensure any suspicious activities are escalated to the relevant authorities. The policies outline the general and minimum standards of internal AML and CFT which should be adhered to by the companies management and employees.

2.1. What is Money Laundering?

Sunrise Worldwide Solution N.V

The purpose of money laundering is to obscure the origin of revenues, which derive from criminal activity. Simply put, the money laundering process occurs when a transaction involving any form of property that has come from any crime takes place. To assist in the fight against ML/FT, the Government of curacao established the National Ordinance Reporting Unusual Transactions (NORUT) and the National Ordinance Identification When Rendering Services (NOIS).

The main aim of money laundering is to disguise the fact that assets involved in a business relationship stem from illegal sources. The process to disguise these illegal funds usually involve a complex system of transactions which are utilised to finally re-introduce the “laundered” or “clean” money into the legitimate economy, disguising the origins of said funds, and making them appear to have come from a legitimate source.

In order to be able to freely spend the money derived from criminal offences, criminals utilise money laundering, and in doing so, distance themselves from a direct link to the funds, whilst retaining ownership, in an attempt to avoid detection by the authorities.

The key identified stages of money laundering are as follows:

- Placement
- Layering
- Integration

Placement

Placement is the stage where the money to be laundered is introduced into the legitimate financial system. At this stage, the funds are still illegitimate thus, the launderer will attempt to incorporate and place the money derived from illicit activity into the banking system to start the process of money laundering. From the Company's aspect, this stage it is very important to understand where the money is being derived from as the person with the intention of committing such an act will need to dispose of the money derived from criminal activity without attracting attention.

There may be several methods for a launderer to perform the placement stage, including the use of cash deposit cheques, traveler's cheques, gambling, loan repayments, insurances on life policies, mixing legitimate with illegitimate funds and asset purchasing amongst other means.

Layering

At this stage the funds have managed to be deposited in the financial institution. Layering is used through complex structures designed to lose all trace of the money and disguise ownership. This may occur by conducting transactions through different jurisdictions. This process is aimed to try to confuse any investigation and mislead traceability of the funds.

Randomly questioning transactions by asking the right questions and avoiding alerting the customer of any wrongdoing, monitoring of transaction and amounts, verification of salaries pegged to a declared position, the use of gambling chips, requesting invoices and comparing declared prices with current market rates, and requesting supporting documentation are all means through which one can verify the source of funds, as well as detect any illegitimate use of funds. These are amongst the few methods of monitoring of transactions used by the Company.

Integration

At this stage the money derived from criminal activity has been made legitimate and placed once again into the financial system, as legitimate funds. At this stage the launderer has been successful in laundering the funds.

The process of money laundering utilises the services of a host of professionals (such as: bankers, lawyers, trustees, accountants, brokers, et), some of whom may be assisting in the process unsuspectingly. Hence, it is imperative for any business having the risk of being exposed to money laundering primarily by way of the services it offers, to implement and maintain policies and producers in place which are compliant with extant regulations and guidelines. Likewise proper implementation monitoring and constant vigilance to these threats need to be maintained at all times.

2.2 Anti-Money laundering policy within the Company

It is Company policy to prevent, detect and report any form of detected attempt of ML/FT occurrences. The Company's policies and governance are designed comply with the extant AML legislations and regulations, as mentioned *supra*, as well as by rules and directives which may be determined from time-to-time by the Curacao FIU, Curacao Gaming Control Board (GCB), and/or any other regulatory body. The Company abides by the examples as illustrated *supra* in its detection of any attempts of money laundering. The Company is committed to aid in the prevention and detection of money laundering attempts, and is also committed to reporting each suspected case to the pertinent authorities for further investigation and action.

2.3 What is Terrorism Financing?

Terrorism financing ("TF") is an additional threat to financial services and businesses. TF is the provision of funds and/or financial support to individual terrorists or non-state actors. The main difference between ML and TF is that the source of funding for terrorist activity is generally lawful. Unlike ML, a relatively small amount of money is required to conduct terrorist activities, which in turn, makes it easier for criminals to evade detection. Many of the techniques employed by criminals to disguise the destination of terrorist funds are identical to those used to disguise the source of illicit funds. Transactions are to thus be monitored to identify in any linkages are to be made with terrorist or criminal activity.

When dealing with terrorist financing, it is important to note that funds do not necessarily have to be derived from criminal activities. The funding of terrorism can adopt a similar methodology to that used for money laundering however the intent and the scope of such acts vary from one another. The Company's standards enforce Customer Due Diligence (CDD) and Know Your Client (KYC) procedures on all transactions. This has made the activity of terrorist financing more difficult for those who are willing to pursue it.

As a "subject person", the Company recognizes the importance of thorough and proper KYC, and has put practices in place to comply with professional standards. The Company has adopted the process of keeping a record of beneficial owners, business entities and the applicants for business, which is constantly updated and kept current, and which shall be further elaborated on below. The lists of individuals and entities are then uploaded and compared daily on an internally built software, which is designed to automatically detect any individuals and/or entities who have been listed on an international sanctions list. Such software is internally designed and maintained.

The software is also programmed to provide immediate notification in case of any changes or new directed individuals or entities included on such a list. Apart from daily monitoring, these controls are also carried out prior to the onboarding of a new customer.

As part of ongoing monitoring of business relationships and/or when notified with a change in beneficial ownership, the Company's compliance team physically check beneficial owners. Where suspicion is raised, the compliance team shall run the search against the internal software, and thereafter, physically check the individuals against the following sanctions lists;

- <http://www.un.org/en/sc/documents/resolutions/>
- <https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list>
- US Treasury Office of Foreign Assets Controls Specially Designated Nationals and Blocked Persons Lists
- EU sanctions lists
- For PEP's: Transparency International Corruption Perceptions Index/
www.knowyourcountry.com

Screening is overseen by the MLRO. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Jurisdiction
- Photo identification
- Identification or passport number
- Place of birth

Where a match is reported, the compliance team shall investigate through open sources to obtain any further information. The MLRO is immediately notified through the extant internal

reporting procedures. The MLRO will thereafter investigate any suspicion, and/or knowledge, and shall report to the pertinent authorities where necessary.

The United Nations (through its Security Council Resolutions) and the EU, may impose several sanctions on both individuals and entities that are known or have been involved to be active in the field of terrorism or funding thereof, and the funding of proliferation of weapons of mass destruction. An example of sanctions followed currently are as follows, saving other sanctions which may be enacted in the interim;

UNSCR 1267 (1999) - Recalling the relevant international counter-terrorism conventions and in particular the obligations of parties to those conventions to extradite or prosecute terrorists, Strongly condemning the continuing use of Afghan territory, especially areas controlled by the Taliban, for the sheltering and training of terrorists and planning of terrorist acts, and reaffirming 'THE COMPANY' its conviction that the suppression of international terrorism is essential for the maintenance of international peace and security and hereby also determining the Freeze funds and other financial resources, including funds derived or generated from property owned or controlled directly or indirectly by the Taliban, or by any undertaking owned or controlled by the Taliban, as designated by the Committee established by, and ensure that neither they nor any other funds or financial resources so designated are made available, by their nationals or by any persons within their territory, to or for the benefit of the Taliban or any undertaking owned or controlled, directly by the Taliban, except as may be authorized by the Committee on a case-by-case basis on the grounds of humanitarian need;

UNSCR 1373(2001) - The Security Council hereby declares that the criminalized the willful provision or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts; and to Freeze without delay funds and other financial assets or economic resources of persons who commit, or attempt to commit, terrorist acts or participate in or facilitate the commission of terrorist acts; of entities owned or controlled directly or indirectly by such persons; and of persons and entities acting on behalf of, or at the direction of such persons and entities, including funds derived or generated from property owned or controlled directly or indirectly by such persons and associated persons and entities;

UNSCR 1718(2006) - Aimed at the security council condemning nuclear tests by democratic people's republic of Korea Member States were bound to act against those activities and freeze the assets of involved entities and individuals of the DPRK. It would provide for an inspections regime to ensure compliance with its provisions, building on the existing work of the Proliferation Security Initiative. `

UNSCR 1737(2006) - Iran's failure to halt uranium enrichment such resolution declares the freezing of assets of those being engaged or directly associated with providing support for Iran's proliferations of sensitive nuclear activities.

Sunrise Worldwide Solution N.V

Council Regulation (EC) No. 329 of 27 March 2007 concerning restrictive measures against the Democratic People's Republic of Korea, whereby instructs that funds shall be frozen, and no funds or economic resources shall be made available whether directly or indirectly or be made available for the benefit of a natural or legal person entities or bodies.

Further regulations consist of EU Regulations implementing these UNSCRs such as Council Regulation (EC) No. 2580 of 27 December 2001, Council Regulation (EC) No. 881 of 27 May 2002.

Further resolutions can be found and updated from, <https://www.un.org/securitycouncil/content/resolutions-adopted-security-council-2019>, such resolutions are in tandem with the current situation or situations of unrest within a particular jurisdiction.

All the above-mentioned regulations and resolutions lead to the following main salient points being:

- All funds are to be frozen (this includes financial assets and economic resources whether owned directly or indirectly by a person or a related entity).
- All those assets being financial or economic resources are not to be made available to or for the benefit of the designated persons or entities.
- If one suspects that a transaction, whether completed or attempted, is related to terrorist financing, he/she should immediately inform the MLRO by following internal reporting procedures.
- If the MLRO knows, rather than suspects, that a transaction is related to property owned or controlled by or on behalf of a terrorist or a terrorist group, he/she shall not complete the transaction and report it to the relevant authority immediately

Note: Details of how any of the above may manifest itself are detailed in the Company's Business Risk Assessment (BRA). The manifestation of risk and the processes are further described hereunder

3. Proliferation Financing

Proliferation Financing (PF) is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. The Company makes reference to the obligations to prevent terrorist activities and terrorist financing which are deemed to be a very high risk to the possibility of loss of life, and additionally refers to the Company Sanctions Policy held internally, which in turn, defines obligations of freezing of assets and reporting.

3.1 Targeted Financial Sanctions

Targeted financial sanctions require countries to immediately freeze funds and assets, and ensure that these funds and assets are not available to or for the benefit of, designated persons and entities. All natural and legal persons (such as the Company), within Curacao, are required to do so without delay. This is to comply with United Nations Security Council Resolutions, and the Common Foreign and Security Policy (CFSP) of the European Union. Compliance with sanctions is mandatory under the Charter of the United Nations. EU Sanctions are binding on Curacao by virtue of the Kingdom Sanctions Act.

The Company has mechanisms in place wherein it can check and act accordingly, where a prospective client has been sanctioned. Further checks along the business relationship are also made, and the relationship is terminated and funds frozen accordingly, if it is discovered that a client of the Company has been sanctioned in accordance to the extant regulations.

4. Anti-Money Laundering Compliance

The Company's terms and conditions highlight our commitment to the applicable laws and regulations. To this end, customers can open an account only once they have indicated their consent with all terms and conditions. The Company monitors all transactions, from the start of the client-Company relationship, and all throughout said relationship, until termination. The Company understands that its most imperative obligations are Customer Due Diligence (CDD) and reporting where necessary.

The Company operates in various ways so as to ensure that it is not conducive and/or is not used as a vehicle for criminal activity.

The Company takes any and all forms of fraudulent activity of players seriously. Fraudulent activity, as determined at the Company's sole discretion, in line with extant legal instruments as elaborated upon *supra*, is strictly prohibited, and is duly reported to the pertinent authorities when detected. Fraudulent activity may include, but is not limited to:

- Stolen credit cards;
- Transfer of funds to other player accounts (chip dumping is currently not permitted and there is no functionality for it);
- Forgery of documentation, collusion (such is not possible at the current stage of operation),
- The use of impermissible software tools;
- The provision of false registration data or other requested information;

In addition to any other provision listed in this policy, and/or the applicable game rules, the Company reserves the right to pursue claims for criminal prosecution and/or civil damages concerning any fraudulent activities, including also, any claims relating to bonus abuse which may constitute as a detriment to the Company.

The Company software does not permit the depositing of funds suspected of originating from criminal activity, depositing funds by using a credit card which a player is not authorised to use, knowingly receiving money from such credit card in any other manner, colluding with a third party to do so, collecting and wagering on behalf of, or using a third party's account with the Company for any criminal activity or illegal purpose.

The Company moreover reserves the right to record telephone calls with players, which may also be used to pass on information to the pertinent authorities for further action including prosecution, should there be any hint of illicit activity. Players involved in any form of suspected fraudulent activity, laundering of funds and/or any involvement in activities related to terrorism and/or any suspicious transaction or activity, will be reported to the appropriate authorities immediately, **upon suspicion.**

The Company's terms and conditions also stipulate that deposits need to be used in full for game-play.

5. The Role of the MLRO

The MLRO is the officer responsible for ensuring that, when appropriate, the information or other matter leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of ML is properly disclosed to the relevant authority.

Operators are required to appoint an MLRO. This task is allocated to the Non-Executive Director, who has to be aware of any suspicious activity that might be linked to money laundering or terrorist financing, and if necessary to report it. This shall be a combined report in which technical as well as responsible gaming information shall be prepared and subsequently reviewed by MLRO.

Therefore, the duties of the MLRO (and deputy MLRO where necessary) shall be as follows:

- Receive reports from the subject person's employees, or through software solutions used to analyse 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.
- Consider these reports to determine whether knowledge or suspicion of ML/FT subsists or whether a person may have been, is or may be connected with ML/FT.
- Report knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the FIU; and
- Respond promptly to any request for information made by the FIU or the GCB.
- The MLRO responsibilities shall also include but are not limited to:

- risk assessment and management;
- ensuring customer due diligence measures and ongoing monitoring;
- record-keeping;
- promoting internal control;
- perform internal auditing of AML/CFT processes (unless internal auditing function is available);
- the monitoring and management of compliance with, and the internal communication of, such policies and procedures;
- monitoring of relevant staff and agent screening;
- Self-education and education of relevant staff in AML/CFT on an annual basis or more regularly if deemed necessary;
- liaison with law enforcement authorities; and
- manage Investigation Order requests received from the authorities.

The MLRO (and deputy MLRO where necessary) report directly to the Board of Directors, within the Company structure.

6. The Risk Committee

The MLRO and Deputy MLRO will be tasked with organising risk committees to discuss pertinent issues in relation to ML/FT. The Committee's members are composed of the Chief Executive Officer (CEO), MLRO, Deputy MLRO & Director. The Committee shall report to the Company's Board of Directors.

Potential or confirmed ML/FT hits will be discussed along with potential threats, typologies and actions/documentation which is to be implemented to address any threats identified.

The Committee will examine the following areas:

- Breach Reporting;
- Ongoing Monitoring;
- Systems and Tools;
- Customer Screenings;
- Transaction Monitoring;
- Trendy & Typologies;
- Business Risk Assessment & Customer Risk Assessment;
- Rules & Responsibilities;
- Policies & Procedures;
- New products or services;
- Business risk assessment.

Breaches of the Company's compliance program are to be immediately reported to the Board. Documentation is to be held in relation to the breach specifically the:

- Type of breach;
- Time of breach;
- Adverse effect of the breach;
- Remediation plan:
 - Actions taken;
 - Actions to be taken.

The above report will have to be signed by the Risk Committee and the board,

7. Risk Assessment

The Company adopts a risk-based approach, in compliance with FATF Recommendations. An AML compliance regime is an essential component of any casino's good governance programme. This ensures that the Company is protected against ML/FT threats and also ensures that the Company is in compliance with all extant laws and regulations. By adopting a risk-based approach, the Company ensures that it is protected and has the capacity to detect ML/FT/PF threats, and that measures in place are commensurate with the risk identified.

In general, the Company adopts the following approach:

- Assesses ML/FT/PF risks which may occur beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the risk identified;
- Monitor and improve the efficacy of these policies, procedures and controls;
- Document the risk assessment, and ensure that all steps are being followed. Adjust steps where necessary in order to ensure a higher safeguard against any ML/FT risks identified.

The risk assessment considers all relevant risk factors, including the geographical location of the player, countries, products and services, and types of games it offers before determining what the overall risk is. The Company also notes the National Risk Assessment (NRA) of the jurisdictions where its services are rendered - this is taken into account when the risk assessment is compiled. Constant monitoring and adjusting is done, as the Company recognises that risks in this business are dynamic.

8. Business Risk Assessment (BRA)

The Company's activity necessitates the conducting of a Business Risk Assessment (BRA) whereby all products/services / verticals and jurisdictions are given due consideration in terms of risk posed. A qualitative and a quantitative approach has been undertaken and the result of which was scrutinised through the application of a quantitative approach, which

assesses the risk posed by the client, products, payment, transaction, interface, employee's and MLRO duties including also internal security.

The BRA is held separately and may be accessed accordingly. For any updates or changes within such assessment a relevant update is provided and for which attendance will be taken, and knowledge of such will be tested accordingly through the following methods:

- Examination/ assessment
- Workshops
- A sampling of work

The policies and procedures are influenced by the BRA, assessing the inherent and residual risk of risk factors and manifestation thereof. As a must, every employee is to be made aware of such policy and the employee's knowledge of the policy is periodically tested.

The BRA is an all-encompassing view of the risks posed to the Company, being: vulnerabilities and threats which may be encountered by the Company through the course of its business, as well as the mitigating factors conducted prior to the seed funding, and continuing on an ongoing basis thereafter, as new or material developments arise.

The residual risk as a result of such assessment will thereby determine whether a particular risk will fall within the risk appetite, or if the risk is too high, so as to outrightly refuse such business. In terms of products, the Company may opt to act so as if the risk falls within a level which is not within the risk appetite, such product's risk mitigators will be increased. If such a product's risk still falls within a level of risk that is not acceptable, the product in question will be discontinued.

A GAP analysis is also conducted to determine any weaknesses to follow through a product offering. The BRA is conducted prior to the launch of any product to identify the risk associated, mitigating factors, and whether such product will fit the company's risk appetite. The factors which are included in the BRA are as follows:

- Product
- Service
- Transaction
- Geography
- Customer
- Interface
- Employee
- Duties of the MLRO
- Third parties

The manifestation of risk of the factors included above are duly assessed in relation to money

laundering and funding of terrorism. In developing the operational AML/CFT procedures set out below, the Company has reviewed its business processes against the criteria set out above with the aim of taking a 'risk-based approach' to the development of AML/CTF controls.

The Company has developed a risk assessment which summarises the areas of low, high and medium risk which it is exposed to, in line with its risk-based approach. The Company has also performed a risk assessment of its operations which are also carried out periodically, dependant on the nature of said risk. For example, due to the evolving nature of technology, risk assessments pertaining to technological products used by the Company shall be carried out yearly, or when new risks or products are in place.

The BRA is updated whenever substantial changes to the Company's systems, processes and overall operations are carried out. It is also re-evaluated, depending on the National Risk Assessment (NRA), as well as based on ongoing monitoring and trends.

The Business ML/FT Risk Assessment and related measures, policies, controls and procedures are to be recorded and made readily available for review by interested authorities, including the Curacao Gaming Control Board (GCB) at any time. All aspects of the BRA are covered, including:

- Methodology adapted
- The reasons for considering a risk factor as high/low/medium risk
- The outcome of the BRA
- Any information sources used.

The BRA is an encompassing view of inherent risks, vulnerabilities and threats to the company, the mitigating factors conducted and the residual risk, and the means and measures employed within which they are mitigated. The company's policies, internal controls, compliance management and procedural documentation, is influenced by the BRA. Every company employee is made aware of BRAs and updates, knowledge of which is tested periodically. The BRA is assessed and approved by the Board of Directors. It is made readily available to the GCB upon request.

The manifestation of risk of the factors above are assessed in relation to ML and FT. In developing the operational AML/CTF policy and procedures, the company has reviewed its business processes against the criteria set out above to take a 'risk-based approach' to the development of AML/CTF controls. The BRA summarises the factors into low, medium and high risk. Due to the nature and evolving technology, the BRA shall be carried out every year unless material changes are noted.

New or material changes shall warrant a re-evaluation of the BRA; such changes shall also be applicable upon introduction of new products, services, jurisdictions and payment methods. Changes within the regulatory framework shall also be considered as pertinent elements that shall contribute to a review of the risk. The business risk assessment is also a criminal risk assessment for which perceived data is taken into account to further prevent any risk from possibly happening. The BRA will be carried out at least annually.

9. Customer Risk Assessment (CRA)

After the identity verification of a client, a risk profile is formed based on the clients' behavioural patterns. This behavioural pattern is examined through the transaction activity and the type of game-play the client opts for. The CRA is also carried out throughout the business relationship.

After the behavioural pattern is analysed, every customer is given an internal classification as defined by the Customer Risk Assessment (CRA). If suspicious behaviour is observed, evidence will be recorded on the customer profile, and Enhanced Due Diligence (EDD) is applied.

Customers undergo an ongoing ML/FT Risk Assessment from the start of the business relationship and thereafter based on:

- customer type;
- products/services used (e.g. sportsbook);
- transactions/payment systems;
- delivery channels; and
- geographical origin of the customer and/or payment method.

Upon registration, a customer's activity will undergo ongoing monitoring through automatic and manual processes to establish a risk profile, which is essential to enable the casino to apply a certain level of Customer Due Diligence (CDD), commensurate to the ML/FT risk posed. This monitoring is maintained, and the risk level may be reconsidered, depending on changes in customer's activity and to establish the point of reaching the relevant due diligence requirements thresholds. A customer's risk profile is key in obtaining relevant information pertaining to the customer, and maintaining a constant diligence on customer risk.

On the basis of the CRA the appropriate level of CDD can be applied, as stipulated in the Client Acceptance Policy (CAP).

10. Client Screening

An overview of the Client screening is provided in this policy; kindly also refer to the PEP, Sanctions and Negative Media Policy for more information.

As a licensed entity, the company recognizes the importance of the customer profile and has in place practices to comply with the laws and regulations concerning identification, verification and screening of the Client for sanctions, political exposure and negative media. Upon initiation of the first deposit within the account registration, the Client will be immediately screened using a third party provider (INSERT PROVIDER) and block any Clients

who are a positive PEP, Sanction or negative media match. Following registration, the company's list of Clients is automatically scanned by (INSERT PROVIDER) on a weekly basis .

Positive matches and those Clients who cannot be discounted as a positive match based on the information obtained through the Company's own manual investigation shall be investigated further through open sources to obtain additional information about the match and immediately inform the MLRO by following internal reporting procedures. The MLRO may appoint anyone within the department to investigate such matters. The Company reserves the right to request further documentation concerning any possible match in order to verify or discount the suspicion. If a positive match is confirmed due to the match meeting several criteria, such matches will be reported to the relevant authority. The following criteria are applicable for a match to be determined as a positive:

- Name and surname
- Date of birth
- Nationality

The MLRO has the responsibility of ensuring that the screening is being carried out as instructed; to achieve this, sampling of the data shall be carried out and recorded accordingly.

9.1 PEP / Sanctions Lists Checks

Customers are also to be screened to confirm that they are not included on Sanctions Lists. Customers are asked on first deposit to confirm whether the customer is him/herself, or is a family member of, or known associate to, a person that is considered a Politically Exposed Person ("PEP") being both domestic or international PEP. The customer is further checked to confirm PEP status once the relevant thresholds are hit, or the customer's profile is considered to be higher than low risk. PEP screening is carried out prior to the initial engagement.

Customers matching any one of these categories are to be automatically considered as a high-risk profile and appropriate measures taken to ensure that the business activity with them is not of an ML/FT nature. Sanctioned individuals cannot be accepted as customers. Refer to **PEP / Sanctions Lists Procedure** and **Customer Acceptance Policy**.

The Company currently conducts manual verification of all users in accordance with its internal procedures, which are carried out by designated Anti-Money Laundering (AML) personnel.

It is the reporting entity's responsibility to perform ongoing checks of its client database against the international lists of designated persons/ entities/ groups to make sure the reporting entity is not permitting/ facilitating access to funds to the ones mentioned on the sanctions lists. The primary sanctions list reporting entities must check against are UN, EU, USA-OFAC lists (expanded below), local lists of all jurisdictions where online gaming and gambling activities are provided and/or clients are accepted, and/or any other lists applicable at present, and/or which may become applicable from time to time.

Instances of sanctions screening:

- during initial client/player registration;
- daily;

The Company shall ensure that it shall not do business with terrorists or suspected terrorists, or other sanctioned persons or companies. Published lists should be checked, being as follows;

- US Treasury Office of Foreign Assets Controls Specially Designated Nationals and Blocked Persons Lists
- EU sanctions lists
- For PEP's: Transparency International Corruption Perceptions Index/
www.knowyourcountry.com

Although due diligence is required for every PEP, as measures required may vary, and the level of diligence is different according to scenarios, such as:

- Type of function carried out by the PEP
- The country from which the PEP originates
- The transactions that the PEP carries out

In the case of PEP's, the termination of the PEP although stipulated at 12 months after resignation, will be assess for further political involvement or possibility of being a close associate with.

9.2 Negative Media

Negative media shall be deemed as information or intelligence, whether proven factual or alleged, related to serious financial crime, Terrorism, fraud, narcotics, or any crime that has an element of or could lead to ML/FT. Negative Media Screening is to be conducted when establishing a business relationship with a Client. Instances where a Client is connected to Negative Media, will be evaluated prior to granting a business relationship.

When analysing Negative Media hits, we are looking at individuals that are both convicted and not fully convicted, meaning; allegations, cases under investigation pending the legal procedure, wanted individuals and any intelligence which gives rise to knowledge or suspicion that the Client is involved with ML/TF.

Negative Media hits showing predicate offences of ML such as mafia, forgery, drug trafficking and fraud and terrorism amongst many others, shall be reported due to the sensitivity of the crime and the involvement of financial crime. Should any predicate offence raise concerns, they shall be raised with the MLRO or Deputy accordingly.

Negative Media is categorised as follows:

Sunrise Worldwide Solution N.V

i) Financial Crime

- Financial crime covers a wide range of activities, including ML and the FT. It may also include fraud, bribery, or insider trading. Financial crime is a broad and complex criminal field that may be covered in both traditional and emerging media.

ii) Violence

- Violence involving Clients directly, or carried out on their behalf, may generate significant different types of adverse media, especially when part of a criminal enterprise. Violent crimes may be associated with political and workforce disputes, or wider patterns of human rights abuse.

iii) Terrorism

- The financing of terrorism, any terror-related activities are liable to generate significant adverse media across a range of media outlets. Terror-related types of adverse media may range from the distribution of terrorist literature and encouragement to radicalization, to the direct perpetration of terrorist acts.

iv) Fraud

- Fraud can be perpetrated in numerous ways and includes fraudulent letters, telephone calls, emails, and websites. Fraud can be both a civil and criminal offence and, while the majority of cases involve improper financial gain, it may also involve property or immigration.

v) Narcotics

- Narcotics crimes involve not only the use or sale of drugs but also drug production and trafficking. Narcotics offences and associated news stories are often related to financial crimes, including ML and FT.

vi) Cybercrime

- Any criminal activity involving a computer or networked device like a phone or tablet may be considered cybercrime and reported as such. Cybercrime is an umbrella-term describing activities used to facilitate other offences like digital financial crime, ML, fraud, and terrorism.

vii) Regulatory

- Regulatory misconduct or non-compliance may constitute a crime in itself, or be an indication that Clients are involved in other types of criminal activity. The types of adverse media stories relating to regulatory offences frequently cross-over with financial crime.

viii) Property

- Adverse media stories on property may involve activities such as burglary, theft, larceny, and arson, and constitute both civil or criminal misconduct. Property offences may vary greatly in scope and be reported in a wide variety of news media formats.

ix) Trafficking

- Trafficking involves the transport of humans for the purposes of forced labour or sexual exploitation. A serious criminal offence, trafficking is often related to other offences, including terrorism and various financial crimes.

x) Sexual Crimes

- Sexual crimes include a wide range of activity, from violence, abuse, and rape to the transmission or possession of illegal imagery. Sexual crimes are often in proximity to other offences, including ML and cybercrime.

Any of the offences indicated above, whether convicted or alleged, shall be evaluated and terminated accordingly if the media is deemed to be a positive match.

11. Risk Factors specific to the Gambling Sector

There are 4 risks which the BRA and CRA cover as a minimum. These are:

Customer risk

This is the risk of ML/FT which arises from maintaining relations with a given person. The assessment is generally based on the individual's economic activity and/or Source of Wealth (SOW). categories of customers who may pose a higher risk are as follows:

- Customers having multiple sources of income
- Customers with irregular income streams
- PEP's
- High spenders (as money can be derived from illegal activities)
- Disproportionate spenders (spending is inconsistent with the Company's knowledge of the individual's SOW)
- Improper use of third parties, use of others to avoid CDD measures and scrutiny
- Unknown customers
- Junkets

To this end, the Company sets an upper value of the customer's probable spending power, which if reached, will trigger further checks.

Geographical risk

This is the risk posed to the Company by the geographical location of the player and the SOW of the business relationship. Nationality and place of residence must be taken into account as the player may hail from a jurisdiction having lax AML laws, and also being a

haven for terrorists. The Company consults the following sources for further information on the risk the player may pose;

- Countries on FATF list of high-risk jurisdictions subject to a Call for Action
- Countries on FATF list of jurisdictions under increased monitoring
- Countries on CFATF public statement
- Countries identified as jurisdictions of concern or primary concern in the US Department of State annual international narcotics control strategy report (INCSR).
- Countries on the European Commission list of third countries having strategic deficiencies in their AML/CFT regime
- Countries sanctioned by OFAC
- Countries identified by credible sources as hosting terrorist organisations within them
- Countries on the corruption perception index (Transparency International)
- The MLRO compiles a list of countries considered as high risk or low risk.

Product, Service and Transaction Risk

Some products are riskier than others, and pose a higher chance of ML/FT occurring through their use, through the use by customers and the acceptance of casinos of specific payment methods. These include:

- Proceeds of crime - money from narcotics, theft etc
- Anonymous payment methods (such as use of Virtual Financial assets etc)
- Use of casino accounts - these are only allowed to be used for gambling purposes and not to withdraw or deposit with minimal play
- Types of specific games (ex: roulette, craps).
- Peer to peer gaming
- Use of customer accounts held in third party names
- Transfer of funds from one account to another
- Identity fraud
- Electronic wallets - not all e-wallets are licensed, and some jurisdictions accept deposits to e-wallets in cash.

The Company employs its best diligence in order to avoid situations such as the above from occurring within its corporation. The Company, together with the MLRO compiles a list of products which are considered as posing more of a high-risk, and employs measures in order to mitigate that risk, accordingly.

12. Risk Assessment - A dynamic approach

Sunrise Worldwide Solution N.V

The Company conducts a risk assessment to assess ML/FT risks whenever a new product is introduced. This is done whenever:

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

In such cases, a risk assessment takes place prior to the launch of a new product, business practice, delivery method, or the use of developing technology. This enables the Company to assess possible risk posed, and mitigate accordingly, or, decline to offer said new product.

Risk management is a continuous process carried out on a dynamic basis. Risk assessment is not an isolated event of limited duration. The MLRO shall undertake regular reviews of the characteristics of existing Clients, new Clients, services and the measures, procedures and controls designed to mitigate any resulting risks. These reviews shall be duly documented as per the Manual's requirements and form part of the company's Annual Money Laundering Report.

13. Customer Due Diligence

The Company does not allow accounts to be kept in anonymous or fictitious names. The Company identifies the player, asks for the player's name, and identifies the purpose for the business relationship. Without sufficient and concrete knowledge, the Company will terminate the relationship. The customer's risk profile is key for the Company to establish and maintain a business relationship whilst maintaining safeguards commensurate to the risk posed. Customer Due Diligence (CDD) is maintained throughout the relationship. This assessment is key in order to identify deviations from any expected behaviour. Any deviant behaviour is immediately reported to the Curacao FIU.

Customer Due Diligence (CDD) Measures include:

- collection of identification details;
- verifying the Identity of the Customer;
- determining the customer profile and levels of activity and adjusting the profile as and when necessary;
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the results of the risk assessment; and
- retention of records of these checks and update them when there are changes.

Casinos have the obligation to undertake CDD measures, when:

Sunrise Worldwide Solution N.V

- players engage in financial transactions equal to or above NAF 4,000.
- Carrying out of occasional transactions equal to or above the monetary equivalent of NAF 4,000.
- There is a suspicion of money laundering or financing of terrorism
- The casino has doubts on the veracity or adequacy of previously obtained customer identification data.

NB: a transaction may be a single transaction but may also be a series or a pattern, equivalent to or exceeding NAF 4,000.

14. Onboarding of New and Prospective Clients

This section describes the criteria for accepting new Clients based on their risk categorisation. Following a risk-based approach for every Client, it will be determined what level of due diligence is to be applied concerning identification, business relationship and transaction level. Where the level of risk is above the level the company is willing to accept, appropriate steps must be taken to mitigate the risk. If the risk cannot be mitigated to an acceptable level, the relationship must be terminated.

The user upon the inception of the account, shall provide the following identification information:

- First name
- Last name
- Date of birth
- Residence address (Building, street, city, country)
- Email
- ID Documentation:
 - Type of ID
 - The Expiry date of the ID
- Nationality
- Place of birth

The company interfaces with Clients non-face to face due to this the company has implemented mandatory verification for which tools and technology will be utilised to limit the risk from non-face to face. The internal controls and compliance management policy shall further indicate the testing of the said methods and four eye approach to further mitigate the risk of non-face to face interaction. The company shall reserve the right to block accounts and request alternative documentation should it be deemed necessary.

In order for the company to know it is dealing with a real person, documentation is required to corroborate as much as the information submitted as possible. The company shall obtain sufficient evidence of identity to verify the person is whom they claim to be (the reader may

wish to note the sections above on CRA)

A Client's residential address is an essential part of their identity, and when it is not present on identification documents, it will have to be obtained separately (once the relevant due diligence level is reached).

The KYC provided will be verified via agents who are trained and who will ensure that the documentation provided corresponds to the information currently held on the Client and that the KYC is valid. If the documentation provided is deemed not to be valid or sufficient, further documentation may be requested from the Client.

Following the risk-based approach, at onboarding, an automated risk assessment of the ML and FT risk posed by the Client is carried out based on the information provided by the Client and checks conducted. The risk assessment will rate the Client as low, medium or high risk, due diligence and ongoing monitoring will be carried out in proportion to this risk (as is explained by this document). If the risk is deemed Medium or High, further information and documentation is required from the Client. If the account is rated High Risk and is exhibiting trends or there is suspicion, knowledge or reason to believe it must be reviewed by compliance personnel and brought to the attention of the MLRO or deputy for approval and analysis.

15. Client Categorisation Criteria

Depending on the Client's category, factors such as the Client's background, type and nature of their business activities, their country of origin and the services they require shall be considered to examine and define their classification. Depending on the level of risk and the customer profile obtained regarding the purpose and intended nature of the business relationship, an adequate level of due diligence is to be applied.

The application of due diligence below shall be determined by risk and thresholds. The below Transaction Limits are deposits into the Client's gaming account, calculated annually from the first deposit over a calendar year (365 day period), with the threshold reset annually.

The customer due diligence (CDD) shall be carried out as follows, in accordance with the triggers and alerts held internally to ensure that the level of due diligence is commensurate with the level of risk of the customer.

Customer Risk Assessed Grade	KYC Level	Requirements	Transaction Limit & possible scenarios
LOW CRA Grade: Is important to notice that clients with a KYC Level 1 will not always be a CRA Low Grade.	Level 1: Simplified Due Diligence onboarding	-- Email - Basic customer information • Official full name; • Date of birth; • Permanent residential address; • Nationality; • Place of Birth - Identity verification (I.D. or Passport) - Selfie Involvement of Virtual Financial Assets - Purpose and Nature of the Relationship • Type of wallet (Dropdown) • Wallet hash • Travel rule details - PEP, Sanction & Negative Media Check - Wallet Verification (chainalysis) (if high or medium follow level 2 and 3 below)	LESS than NAF 4000 Even if the operation stays below NAF 4000, the CRA Grade could be Medium or even High, in accordance with the results of the screenings and searches upon inception, as well as if the Customer triggered any alert on the risk score or transaction monitoring tools.

Sunrise Worldwide Solution N.V

MEDIUM CRA Grade: Is relevant to notice that clients with a KYC Level 2 will not always be a CRA Medium Grade.	Level 2: Customer reaches NAF 4000 in deposits, due diligence is mandatory.	- Above, plus - 7 basic SOF/W questions being: • Status of employment • The expected volume and frequency of transactions • Proof of income (dropdown from SOW/F) • Gross annual income • Proof of ownership of the wallet • Profession (non-CAP list and Client has to declare that they are not involved) - Proof of address document	1st scenario: Customer exceeding NAF 4000 or equivalent . 2nd scenario: CRA Grade is considered a medium after the screenings and searches upon inception, even if the customer got a KYC Level 1 upon inception. 3rd scenario: Customer (KYC Level 1) triggered an alert on the risk score or transaction monitoring tools that placed the Customer in a Medium CRA Grade..
HIGH CRA Grade.	Level 3: Enhanced Due Diligence onboarding	- Above, plus - Additional SOF/W: • Proof of Income documents including SOW/F (Verification through documentation)	1st scenario: reaching the annual limit. 2nd scenario: The Customer was considered KYC Level 1 or 2, however a high alert on the risk score or transaction monitoring tools were triggered, then the Customer is a High in the CRA Grade. See

			Transaction risk (monitoring) alerts in the Risk Assessment excel file. 3rd scenario: Client reached expected level of activity or deposits client has reached 15,000 euro deposits in one year or 45% of the gross in the income is less than 15,000 euro or equivalent annually
--	--	--	--

15.1. LEVEL 1

Level 1 customers will only be able to transact up to a maximum aggregate value of less than NAF 4000 cumulatively or in one lump sum, Level 1 consists of the provision of the customer's:

- Full name
- Date of birth
- Permanent residential address
- Email address
- Age
- Sanctions and PEP searches

Identification document:

- A valid unexpired passport.
- A valid unexpired national or other government-issued identity card.
- A valid unexpired residence card.
- A valid unexpired driving licence; or,
- Other documents containing photographic evidence of identity that are not government-issued but which are nonetheless recognized as a legal means of identification by the national law of an EU or a reputable jurisdiction.

The client shall be also instructed to provide a:

- 3D liveness check or portrait photograph ("selfie")

15.2. LEVEL 2

Level 2 consists of the requirements laid down in Level 1 and the verification of that information through the provision of the following document:

Verification of address is carried out to

- A recent utility preferably not older than six (6) months;
- A recent statement preferably not older than (6) months, from a recognised credit institution;
- Correspondence from a central or local government authority, department or agency;
- A record of visit to the address by a senior official of the subject person;
- Any identification document where a clear indication of residential address is provided; or
- Certificate of conduct issued by a law enforcement authority.

Should the customer risk assessment indicate that a customer poses a medium level of risk, the customer will be subjected to Customer Due Diligence (CDD) requirements.

Level 2 CDD will be applied for customers transacting with an aggregate value of that is equal to or more than NAF 4000s, or in those situations where the risk assessment indicates that the customer is likely to carry some risk towards and Level 2 and 3 are manually prompted: The information to be provided by the customer at this stage shall be:

- Status of employment
- Proof of Income (SOW/F) (dropdown unless High Risk source of income)
- Declaration that customer is not involved in any activity prohibited by the CAP- we draft it, and customer accepts it (yes/no)
- Annual expected activity in NAF
- Gross annual income (source of wealth and funds)
- Jurisdiction of SOW/F (dropdown and back office to upload the proof of income document)

IF customer chooses SOW/F that prompt mandatory verification, the customer will be prompted to upload the proof of income document, and such is to be verified manually by the fraud prevention department

15.3. Level 3

Level 3 is subject to the risk assessment and pre-threshold assessment, for which, if the customer risk is not that of a low or medium, Level 3 will be immediately deployed holding

all information in Level 1 and 2 accordingly. Level 3 shall contain all verification of the source of wealth and funds

15.4. Origin of source of wealth and funds

To establish the source of funds and source of wealth used in a relationship with a customer can usually be established upon review of the transactions of the economic activity from where the Client obtains such funding is in line with Clients original net worth.

Note: Corporate crypto wallets are not an acceptable source of account funding.

Below is sample documentation to be requested in the SOW/SOF process. Note for each of the funding sources below, before the 'Additional evidence, if required' bullet point the mandatory documentation required for that particular funding source is shown. In order to avoid confusion, the mandatory documents will be marked with 'Mandatory':

- **Salary income:**
 - 3 month bank statement(s) showing receipt of salary (Documentation is to be 3 to 6 months old) **(Mandatory)**.
 - **Additional evidence, if required:**
 - Original or certified copy of a payslip (or bonus payment);
 - Letter from employer confirming salary on company letterhead; or
 - Copy of tax return annual statement.
- **Company profits:**
 - Distribution of dividends certificate **(Mandatory)**;
 - Certificate of incumbency (if we can upload 2 documents) **(Mandatory)**; and
 - Bank statement clearly showing receipt and origin of the dividends (Documentation is to be 3 to 6 months old) **(Mandatory)**.
 - **Additional evidence, if required:**
 - Latest audited accounts (if self-employed/own company) and company bank statement for the past six (6) months;
 - A declaration from a certified accountant stating that the company is held in good standing order, confirming dividend, share capital and profits generated. The letter shall include a declaration of beneficial ownership of the company;
 - Certificate of incumbency; or
 - Copy of invoices showing trading activities of sales and purchases.
- **Sales of shares or other investments/liquidation of investment portfolio/bonds:**
 - Bank statement clearly showing receipt of funds and investment company name or interest on bonds received (Documentation is to be 3 to 6 months old or the period of the sale if it exceeds 6 months) **(Mandatory)**.
 - **Additional evidence, if required:**

- Certified investment/savings certificates, contract notes or cash-in statements.
- **Sale of property:**
 - Copy of contract of sale **(Mandatory)**; and
 - Bank statement showing proceeds of the sale (Documentation is to be 3 to 6 months old) **(Mandatory)**.
 - **Additional evidence, if required:**
 - Bank statement showing proceeds of the sale; or
 - A letter from a licensed solicitor or regulated accountant stating property address, date of sale, proceeds received, and name of the purchaser on letter-headed paper.
- **Sale of the company:**
 - A Letter detailing company sale signed by a licensed solicitor or regulated accountant on letter-headed paper **(Mandatory)**; and
 - Bank statement clearly showing receipt of the sale and origin of the funds (Documentation is to be 3 to 6 months old) **(Mandatory)**.
 - **Additional evidence, if required:**
 - Copies of media coverage (if applicable) as supporting evidence.
- **Inheritance:**
 - Copy of the deceased's will **(Mandatory)**; and
 - Bank statement(s) showing receipt of funds (Documentation is to be 3 to 6 months old or the period of the sale if it exceeds 6 months) **(Mandatory)**.
 - **Additional evidence, if required:**
 - Signed letter from a licensed solicitor or estate trustees on letter-headed paper;
 - Grant of probate (with a copy of the will), which must include the value of the estate.
- **Loan:**
 - Copy of the loan agreement **(Mandatory)**; and
 - Bank statement(s) showing receipt of of the loan (Documentation is to be 3 to 6 months old or the period of the sale if it exceeds 6 months) **(Mandatory)**
 - **Additional evidence, if required:**
 - A copy of the identification documents of the individual/s granting the loan; or
- **Gift (exception: 3 mandatory documents):**
 - Letter from the donor explaining the reason for the gift and the source of the donor's wealth **(Mandatory)**;
 - Certified identification documents from the donor **(Mandatory)**; and
 - Bank statement showing the origin of the gift payment clearly (Documentation is to be 3 to 6 months old or the period of the sale if it exceeds 6 months) **(Mandatory)**.
 - **Additional evidence, if required:**
 - The donor is to provide identification documents from the following:
 - Passport or national identification document; or

- Portrait photograph ("selfie") of donor holding their identification document;
 - Bank statement clearly showing receipt and origin of the gift.
- **Fixed deposit – Savings:**
 - Savings statement **(Mandatory)**.
 - **Additional evidence, if required:**
 - Evidence of account start, either; a letter from the account provider or the first statement; or
 - Additional evidence showing the origin of the savings held.
- **Funds generated from gambling/gaming winnings (exception: 2 documents):**
 - Receipt of winnings **(Mandatory)**; and
 - Documentation (e.g. bank statement) showing the origin of the funds which were initially deposited **(Mandatory)**.
 - **Additional evidence, if required:**
 - Bank Statement showing the winnings being received and their origin.
- **Pension:**
 - Bank statement showing the release of pension payment and indicating the name of the pension fund making said payment **(Mandatory)**.
 - **Additional evidence, if required:**
 - Copy of the pension statement.
- **Mining:**
 - Ledger of the amount of cryptocurrency mined **(Mandatory)**; and
 - Wallet address and transaction hash to which the mined cryptocurrency was delivered **(Mandatory)**.
- **Crypto-Investments**
 - Ledger of trades and initial investment **(Mandatory)**

Example

Q: The Client presents a bank statement being used to deposit funds into their crypto wallet, which is being credited by another bank account held by the Client. The account funding source has not been established e.g. salary.

A: In this instance one should seek to obtain:

1. The bank statement from where the funds are being deposited showing the incoming funds
2. A copy of a payslip
3. A copy of the tax returns for the previous year (optional to be used in cases where tax evasion is suspected)

In any situation, the origin of the funds is to be established. If salary is the funding source, we need to see the salary deposit on the bank statement.

Our focus during the SOF/SOW request shall be to understand how the Client funds their transactions therefore until this is sufficiently understood further documentation and

information shall be requested. We must document and keep on file our investigations into the Client's SOW/F, including any questions asked, responses received and supporting evidence provided, which must be updated on an ongoing basis. If our team has any concerns about the source of funds, we must consider whether we need to submit a SAR to the MLRO.

15.5. LEVEL 3

It is pertinent to note that the Level 3 is the highest level of due diligence held on the customer. Level 3 shall be mandatory and shall be deployed when:

- The customer has exceeded the threshold set on the account
- If the customer has triggered any transactional or fraud triggers. See Transaction risk (monitoring) alerts in the Risk Assessment excel file
- The Risk assessment is that of a High
- Customer is from or has links to a high risk or non-reputable jurisdiction
- If any of the above are triggered, then the execution of Level 3 is mandatory. The requested documentation within this level is the verification of the source of wealth and funds
- Provision of a valid, recent proof income document detailing the wealth and funds of the customer as required on a case-by-case basis.
- Provision of further source of funds information should it be necessary to verify the transactions to be conducted by the customer.
- Provision of a valid, recent proof residential address document.
- Profession or Occupation

The threshold has been devised so no customer will exceed NAF 4000 or equivalent without prompting Level 3 due diligence. Should the customer not provide the information, the customer will not be able to further use the platform. The system shall deploy Level 3 automatically or in those cases where it is manually prompted by the agent reviewing the account.

In those cases where the customer is manually prompted and does not reply within a 30-day timeframe, such cases will be escalated for further investigation, for which if warranted an SAR/STR will be raised.

In those cases where the trigger is done automatically, hence stopping the customer depending on the source of income chosen, thresholds and risk assessment. Should the customer not reply to the said information request, the account will be automatically blocked within 30 days and the funds are to be sent back stating failure to provide CDD documentation the block shall be of withdrawal within those 30 days and a hard block after. There should be an analysis and a record kept (via Excel) of the review of the account and why no SAR/STR has been raised. This data will also serve to know the number of accounts being blocked.

16. Measures relating to CDD- Procedural Controls

CDD measures are to be taken as follows:

- Identifying the player and verifying that the customer's identity, using reliable independent sources, documents, data or information
- Identifying the beneficial owner and taking reasonable measures to verify the beneficial owner such that the casino is satisfied that it knows who the beneficial owner is
- Understanding and obtaining information on the purpose and intention behind the business relationship
- Conducting of ongoing due diligence on the business relationship and scrutiny of transactions undertaken are consistent with the Company's knowledge of the player, business risk, as well as source of funds.

The Company and its employees will not disclose that a report has been passed on to the FIU for further processing, as this is commensurate to "tipping-off" which is a criminal offence. If the Company and/or its employees fear that performing CDD will act as a tipping-off to the suspect customer, a report should be raised to the FIU in lieu of performing CDD.

The Customer Due Diligence Procedure defines the procedure used to carry out Customer Due Diligence including timeframes and/or values, when this will be triggered and in which cases Enhanced Due Diligence (EDD) will need to be performed (ex: if a transaction raises a suspicion of money laundering). CDD is necessary in order to enable the casino to apply a certain level of due diligence in order to mitigate ML/FT risks. Any unusual behaviour is to be immediately reported by the subject person to the Curacao FIU, and the latter may decide to proceed accordingly, with further steps, including prosecution.

Depending on the customer's risk profile, customers who have been requested to complete the CDD Procedure may have their account restricted during this period.

The following also lists key points when conducting CDD:

16.1 Identification and verification of the player:

Identification refers to the collection of personal details of the player used to establish the identity of said player. When identifying the player, the following information should be collected:

- Full name
- Permanent residential address
- Date of birth
- Place of birth
- Nationality
- Identity number

In low risk scenarios, it may be acceptable to obtain details from (1-3). In high risk scenarios, additional personal details may be obtained.

16.2 Carry out a customer risk assessment

This is done to have sufficient information available to detect unusual activity in the course of the business relationship. At this stage, a provisional risk rating will apply. This is revised once further information is obtained. On the basis of the Customer Risk Assessment (CRA), the proper level of CDD can be applied, as stipulated by the Customer Acceptance Policy (CAP).

16.3 Verification of identity

This usually takes place on the basis of government issued documentation containing photographic evidence (passport, identity card, etc). where such a document does not include the residential address, the Company requests other documents (utility bill, rental agreement, bank statement). Verification can further be made by checking on social media, telephone directories, company registries etc. Verification is carried out by the casino to assure itself that the customer is who he purports to be. If the casino obtains foreign documents extra care should be taken in order to verify its authenticity.

The customer will be given a timeframe within which all requested documentation shall be provided. Should the CDD Procedure not be completed within the established timeframes the customer's account will be considered to have failed completing CDD and thus will be denied from any further activity. The raising of a Suspicious Transaction Report ("STR") is to be considered. Such a decision is to be taken and recorded by the MLRO.

Unless a STR has been raised and an appropriate period has passed in which the customer has still not completed CDD, the account may be closed, and deposited funds still present on the customer's account will be returned to the deposit method, where possible, less any charges incurred by the business for transmission to this destination.

17. Obtaining information on the purpose of the business relationship

This is one of the requirements of CDD – the development of the customer's risk profile to have sufficient information available to allow for the detection of unusual activity.

Where the risk is not high, a salary statement with some details (ex: nature of employment) can be sufficient. Social media can also be used as a source of information.

When the risk of ML/FT is higher, a casino may require that the information is backed-up by independent and reliable sources, such as information from the Central Statistics Department, such as: average national income, average disposable income, etc. These pointers will allow a casino to discover wagering power amongst jurisdictions.

18. Ongoing and Transaction Monitoring

Sunrise Worldwide Solution N.V

Ongoing monitoring is an intrinsic part of the Due Diligence process. It must be performed on all matters, regardless of the risk rating of the Client, to detect unusual or suspicious transactions. The primary objective of ongoing monitoring is to:

- The scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions being undertaken are consistent with the subject person's knowledge of the customer, his business and risk profile, including where necessary, the source of funds and that the funds are obtained from legitimate lines of business and not any business within the Customer Acceptance Policy and
- Ensuring that the documents, data or information held by the subject person are kept up to date.
- Keep- up-to date information used for CDD or EDD purposes (identity and verification documents); (the system will alert those instances where the documentation is about to expire);
- Stay alert to changes in the Client's risk profile and anything that gives rise to suspicion; and
- Monitor transactions for possible indicators of ML/FT.

The company shall examine, as far as reasonably possible, the background and purpose of all transactions that fulfil at least one of the following conditions:

- complex transactions that have no apparent economic or visible lawful purpose;
- large transactions that have no apparent economic or visible lawful purpose;
- unusual patterns of transactions that have no apparent economic or visible lawful purpose; and
- transactions which are particularly likely, by their nature, to be related to ML/FT.

A manual review of the account can be conducted at the CDD threshold to ensure the client is properly assessed. Open source intelligence is also to be used and to corroborate SOW/F information provided this shall be carried out on those clients for which have raised concern in relation to the funding of the account or upon review. If there is a mismatch between the information provided by the Client and background research, this could lead to a ML/FT concern leading to the Client being risk-rated High and SOW/F documentation requested to corroborate SOW/F information provided.

Ongoing monitoring can trigger a further risk assessment of the Client due to transactional alerts, and if transactions are involved in the alert, they will be scrutinised to establish whether any suspicious activity or transactions are occurring.

A full review of the account will be conducted being as stated both on the identification and verification information and the transactions. A note shall be left on the system detailing what has been checked and the result of the checks carried out. Accounts can have their risk ratings increased via override, such will indicate that the account is to be reviewed more frequently.

Periodic Ongoing Monitoring

Accounts shall be periodically reviewed from the date of the last CRA based on the Client's level of risk:

- High Risk: 12 months
- Medium Risk: 24 months
- Low risk : 30 months

The above time frames are a backstop for when an account review is required. If the Client triggers before and a review is conducted, the periodic review timer restarts and is set from the date of the last Client review.

19. Timing of CDD Measures

A verification of identity is done when a customer engages in a transaction equal to or exceeding NAF 4000. All CDD measures would have been done when that threshold is reached. A minimum level of CDD is compiled prior to reaching that threshold.

Simultaneously with opening the account, the Company verifies the identity of the customer (as described above), and also conduct sanction/PEP screening. Once the threshold is reached, PEP screening is once again initiated, and a CRA is conducted. EDD is also carried out. The reader is invited to *vide* the explanation of EDD carried out by the Company.

Due Diligence must be carried out:

- Before establishing a business relationship with a Client. Due Diligence is to be conducted before allowing the Client to do any transaction of deposit funds onto the platform;
- Before carrying out a one-off transaction for a Client, i.e. those Clients who access the platform and conduct one transaction (which be treated as a business relationship);
- Where there is a reason to believe that Due Diligence carried out on an existing Client is inadequate;
- Where the Client's identifying details e.g. name or address, have changed;
- Where the Client has not been in regular contact with us;
- Where someone is purporting to act on behalf of a Client;
- Where suspecting ML or FT Client may be requested further documentation;
- Where the Client reaches the established thresholds
- SOW/F identification and verification shall be re-conducted periodically according to the Client's level of risk. High Risk Clients shall have SOW/F re-verified every 1 year and Medium risk clients every 24 months.
- EDD must be carried out when any of the situations in the 'Mandatory Enhanced Due Diligence' sub-section above occur.

Sunrise Worldwide Solution N.V

20. Identification and verification of the Beneficial Owner

Identification relates to the collection of personal details. Verification relates to the confirmation of the veracity of said details. When identifying the player, the list as stipulated above on “identification of the player” should be followed.

The Company shall ensure that the account is used by the individual having opened it. This is done through explicit wording in the terms and conditions which the player is made to accept upon registration, including that the player is going to play on their own behalf, lest dire legal consequences arise, should the player be caught as having falsely accepted these terms. Ongoing monitoring from the Company’s end shall ensure that these terms and conditions are being responsibly adhered to.

21. Enhanced Due Diligence (EDD)

A risk based approach shall be undertaken, moreso for high-risk customers. EDD is conducted in several scenarios, such as:

- Residents of higher-risk geographical areas
- PEP’s
- Products or transactions which may allow anonymity
- New products and business practices where the risk has not been sufficiently gauged, and further examination is required.

Applied measures tally with risks identified, such as:

- Obtaining additional information on the customer’s occupation, previous address, and official information (such as info held on governmental databases)
- Obtaining additional information on the intended nature of the business relationship
- Obtaining additional information on SOW/F
- Obtaining information on the reason behind transactions (intended/performed)
- Obtaining additional clearance from higher management to continue with the business relationship
- Enhanced monitoring of the relationship
- Requiring the first transaction to be carried out through a bank with similar CDD standards.

22. Mandatory Enhanced Due Diligence

- EDD will be conducted in the following situations
- Clients with multiple revenue streams for which are not easily identified where the provenance of funds is aminating from;

- Clients receiving funds to or from high-risk or non-reputable jurisdictions as per internal jurisdiction risk assessment.
- Clients who are from a high risk or non-reputable jurisdictions as per internal jurisdiction risk assessment (See the 'Jurisdiction Risk' section for more information on which jurisdictions are high risk);
- The Client attempts to deposit more than the allowed 45% threshold based on the users Gross Income;
- If at the time the NAF 4000 threshold is reached, the Client is rated as medium risk (CDD), then the Client is only temporarily rated as a High Risk (EDD) until SOF/SOW is verified, at which point the Client goes back to medium risk (CDD). If the Client's SOF/SOW is not verified the account is suspended and the Client will remain on the EDD level. The Client if they wish to re-activate the account will have to provide SOF/SOW verification documentation;
- SOW/F shall be re-verified periodically according to the Client's level of risk High Risk Clients shall have SOW/F re-verified every 12 months.
- A manual review of the account is conducted inline with CDD and there is a mismatch on the SOW/F information provided by the client and background research. SOW/F verification is required to corroborate the information provided by the Client.
- Accounts following CRA has resulted in a High Risk;
- Accounts with a suspicious transaction pattern; or
- The Client is a PEP.

Clients at the CDD level shall be rated EDD temporarily until the SOW/F shall be requested if either of the above thresholds are reached. Once the client provides the relevant information the 45% threshold will be calculated on the verified amount of the client's SOW/F.

We can only request information from the Client which assists us in addressing a concern or understanding how the Client is financing their activity. The information required from the Client changes based on the changes in legislation in the different regions. Requesting more information will result in a legal defence.

If a Client refuses to provide any information or fails to provide the necessary information within the relevant time period, we will suspend the account and stop processing transactions. The case shall be raised further with the MLRO or designated individuals assigned to decide whether the case warrants further reporting to the relevant authority by analysing activity to identify knowledge, suspicion or reason to believe ML/FT.

23. Simplified Due Diligence

Simplified Due Diligence (SDD) is employed where the risk of money laundering is lower. Measures include:

- Obtaining only the player's identity (if the risks presented is lower)

Sunrise Worldwide Solution N.V

- Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship - the extent of verification depends on the nature of the business relationship. In a low-risk scenario, bank statements, birth certificates etc may suffice.
- Reduction of the degree of monitoring, whilst still allowing for diligent monitoring.

The Company applies CDD measures to existing customers, on the basis of materiality of risk. The Company performs CDD regularly, at a minimum once yearly, depending on risk level. The Company evaluates whether the measures in place are sufficient to provide for appropriate CDD. In the case that the Company deems such measures to be sufficient, CDD is applied, and care is taken to ensure on-going monitoring obligations, as detailed above.

24. Termination of the business relationship

In the event that the obligations mentioned in the CDD measures section above cannot be met, the Company shall refrain from establishing a business relationship and/or a transaction with a given customer. In such a case, the Company shall block any further transactions and terminate the business relationship.

In a situation where the customer provides the requested information after the account is blocked, the Company's risk department shall assess whether the delay affects the ML/FT risk within the company vis a vis the given customer. The risk department shall also seek the feedback of the MLRO in such a situation. In the case where a suspicion of ML/FT exists, the Company shall file a report with the FIU.

If there is no reason to retain funds, these funds can be remitted back to the customer via the original payment method.

25. Reliance on third parties to perform CDD

The Company may elect to outsource its CDD function to a third party. The third party shall be subject to CDD and record-keeping obligations. The third party shall have a business relationship with the customer, independent of the relationship between the Company and the customer. The Company understands that the ultimate responsibility for CDD measures depends on the Company.

The criteria for such a relationship to be established shall be as follows:

- The Company has to obtain information concerning elements a-c of the CDD measures described above from the third party
- An agreement with the third party that copies identification data or other requested information relating to CDD requirements will be made available on request.

Nonetheless, the Company understands that ultimate responsibility for conducting a CRA, determining whether a customer is a PEP and ongoing monitoring rests with it.

- Shall ensure that the third party provider is duly regulated, and has a proper functioning system where to conduct CDD.
- Regular periodical assessments of how the third party is conducting CDD and ensuring that this is done in accordance to extant practices.

The Company understands that ultimate responsibility for a correct procedure lies with it.

26. **Payment Methods**

The Company will not accept to receive or make cash deposits or payments in relation to customer's activities.

The Company will only make use of payment methods that are:

- **Bank transfer**
- **Credit card**
- **Crypto**

The Company will hold received payments from customers into a player's account, distinct from Company accounts.

The Company will always keep track of transactions carried out using these payment methods and identify funds that are received or remitted by customers, together with any transfers of funds that are made into or out of the player's account for settling the customer's remote gaming activity. It will also be able to identify when thresholds for due diligence have been reached.

In all instances, where possible, funds returned to customers shall be returned to the customer's originating payment method. If this is not possible due to the nature of the payment method or in case of the account not being available any more to receive funds, payments will be transferred only to a bank account in the customer's name, following completion of the customers' due diligence process.

Transaction monitoring will be carried out internally by the AML/CFT monitoring staff also supported by triggers and controls currently inbuilt in the system.

27. Notifications of Fraud, ML/FT, and Law Enforcement or Regulatory Authorities' requests

The Company understands and adheres to its obligations under the NOIS as well as other extant laws, relating to notifications of fraud, ML/FT and reports to law enforcement.

The Company has adequate procedures in place which cover the following:

- The recognition of unusual transactions
- The documentation of unusual transactions
- The reporting of unusual transactions.

The Company will record and take appropriate actions whenever a notification of fraud or requests by Law Enforcement or relevant Regulatory Authorities are received, such as the Curacao FIU. The Company will follow a due process to ensure such notifications or requests are processed without delay and the Company will, within its abilities, assist such authorities effectively.

28. Reporting Obligations

The Company shall detect and report intended and/or completed unusual transactions. The Company has the following steps in place:

27.1 Recognition of unusual transactions:

This means a transaction which is inconsistent with the player profile, based on the information gathered during the course of the relationship. Based on NORIUT legislation, objective and subjective indicators have been established as a means of which the Company must assess whether a transaction qualifies as an unusual transaction. All such transactions must be reported to the compliance officer in charge, and shall be kept on file and reported to the FIU. If not reported, the reason as to why must also be documented.

Unusual transactions may qualify as the following:

- Transactions which in connection to ML/FT are reported to the police
- Transactions on behalf of a person or entity named on a list adopted by virtue of the Sanctions National Ordinance (NG 2015 no.55)
- Transactions in the amount of NAF 5000 or above regardless of the means of the payment (including cash-outs) – this may be done by way of a single transaction or a series of transactions amounting to NAF 5000, a cashless transaction in the amount of NAF 5000 or above, sale to a customer of chips in the amount of NAF 5000 or more to be done in one gaming session..

Reporting of unusual transactions:

In accordance to Article 11 of the NORUT, the Company must report any unusual

transaction to the FIU. In this case, the MLRO shall report any noted unusual transaction to the FIU without delay. To that end, the compliance officer having noted an unusual transaction shall immediately raise this with the MLRO. Supporting documentation shall also be provided.

29. Suspicious Transaction Report

An internal Suspicious Transaction Report (STR) is to be sent directly to the MLRO whenever there is a suspicion that a customer is engaged in ML/FT.

No one is to divulge to co-workers, line managers and especially the customer/s that an STR has been raised as this is potentially considered to be 'tipping-off'. An employee who raises an STR must escalate directly to the MLRO.

Refer to the Internal Suspicious Transaction Report Procedure for guidance on STR escalation.

30. Prohibition of Disclosure

The Company and its employees shall in no way disclose any report raised to the FIU, as this is conducive to "tipping off" which in and of itself is a crime, and will jeopardise the effective analysis and/or investigation into ML/FT. In this sense, caution is advised against the immediate termination of a business relationship with the a suspected customer, as a termination may, in a way, raise suspicion - in such a case, the Company adopts the policy of increasing ongoing monitoring whilst reports are submitted to the FIU, so there is no risk of a potential criminal investigation being in any way, affected.

31. Record-keeping

The Company maintains full transaction records for a minimum of five (5) years (or longer if requested to do so by the pertinent authorities), after a relationship has ended or a business transaction terminated.

The Company maintains records pertaining to CDD (ex: passport copies, ID cards, utility bills etc) for a minimum of five (5) years (or longer if requested to do so by the pertinent authorities) after a relationship has ended or a business transaction terminated.

32. Employee training

Within an appropriate period of the commencement of employment, employees are to be provided with ML/FT training to ensure they are aware of measures, policies, controls and procedures that are in force. Employee training shall be in line with the indicators established through the Ministerial Decree regarding the Indicators for Unusual Transactions (NG 2015 no. 73). This training shall include:

- General awareness of Money Laundering / Terrorism Funding for all employees
- Specific Guidance on the related measures, controls, policies and procedures in

place within the company for employees specifically occupying roles related to AML/CFT Controls and Compliance

- Explanation on CDD, subjective and objective indicators for reporting unusual transactions.
- An assessment to ensure that the employee has grasped the key points of training received.
- The training provided to employees is to be recorded and refreshed at least annually.

The MLRO is also required to attend annual refresher training and to keep up to date with the subject.

Further information about employee training may be found in the Human Resources' relevant policies and procedures.

33. Employee screening

The Company's prospective employees that are to be involved with or connected to activities that would fall within the scope of this policy, are to be screened before they are employed. The Company is to ensure that they are fit and proper to occupy positions in which they will participate in the provision of services to the customer. The use of third party screening providers may be engaged to ensure this.

The Company will carry out monitoring of the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the Company's operations and obligations. The Company will at all times do its utmost to respect the privacy of its employees.

Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the MLRO and / or Directors directly and should they wish to remain anonymous, to do this via an anonymous letter or email service providing as much facts and information as possible.

Further information about employee screening may be found in the Human Resources' relevant policies and procedure

34. Risk Appetite

The company currently has a high-risk appetite when it comes to customer acceptance however, a medium risk appetite in relation to business risk meaning that the residual risk of any product or service has to have sufficient controls in place to mitigate such risk to be within controllable boundaries and for which the company has control over the behavioural pattern and relationship with the Client.

The policies and procedures hereunder reflect such concepts and are therefore in place to further activate the desired result in ensuring proper risk management and mitigation. The company has a

policy concerning Risk Appetite which includes the tolerance for every section of the business, which is approved by the board of directors and reviewed annually for any changes.

Kindly also refer to the document entitled Risk Appetite Statements, which provides a comprehensive understanding of the risk level the company is willing to undertake depending on the scenario.

35. Customer Acceptance Policy

Customer acceptance policy – ‘CAP’. Kindly refer to Customer Acceptance Policy documentation for more information.

The Customer Acceptance Policy (“CAP”), following the principles and guidelines described in this Manual and the CAP document, defines the criteria for accepting new Clients and defines the Client categorization criteria which shall be followed by the company, as well as, and especially by, the employees who shall be involved in the Client acceptance and processing procedure for the provision of the services.

The company has a high-risk appetite for customers, which can only be entertained via controls and risk mitigation not only with the application of ‘EDD’ following a risk level criteria and procedures within the organisation, but also by identifying risks posed with the product and by continuous monitoring and strengthening controls within the company. through the BRA.

It is pertinent that the Customer Acceptance Policy is followed at all times, due to the company being a subject person, the Curacao AML/CFT laws must be strictly adhered to. The CAP provides a better understanding of those customers the company is engaging with and those customers who, due to prohibited actions, risk awareness, sanctions or who display characteristics described in the Sanctions National Ordinance (and any amendments as may be promulgated from time to time) the company will not engage in any activity with.

The scope of this policy is not to turn away customers who shall be deemed to be “genuine”, as the rate of acceptance is the income source of the company. It is therefore essential to adhere to international and local legislation as not all individuals seeking to establish a business relationship may be able to do so due to the risk the said individual will be likely to bring towards the company.

The COMMISSION STAFF WORKING DOCUMENT along with the REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the risk of ML and FT affecting the internal market and relating to cross-border activities has been reviewed and an assessment carried out in this policy.

The result of the latest national risk assessment can be found on FIU website and is accessible through the following link:

<http://www.mot.cw/web/motweb/motweb.nsf/lookupnews/8386911FE53AC62C042589B10071D165?OpenDocument>

Clients who do not comply with the due diligence procedures or are deemed to try to bypass such shall not fall within the CAP. Clients who engage in illegal activity or trigger any of the established rules within the company setup shall be reviewed for malicious practice and if intent is established, such individuals are not considered to be within the acceptable limits of the company. The below sections provide details of situations in which the company outright refuses to do business with a Client.

The CAP shall be predominantly determined by the risk assessment carried out on the Client. The company shall refuse Clients who do not fall within the acceptable risk appetite or in those instances where the Client is linked or involved in a line of business, as indicated below. In the risk sections of this document, there is a clear analysis of how the company conducts risk assessments and the actions undertaken in each scenario to address identified risks. High-risk customers must be approved by the MLRO who will indicate the steps to be undertaken with the said Clients including the mandatory completion of all EDD obligations until any suspicion is cleared and a true understanding of the customer profile is obtained.

The scope of the CAP is to:

- Manage any risk that the company may be exposed to through the provision of its services to customers;
- To prevent the company from being used, intentionally or unintentionally, for ML and/or FT purposes; and
- To identify customers who are likely to pose a higher than average risk

Sunrise Worldwide Solution N.V

36. Reporting to the FIU

The company takes any form of illicit activity very seriously. Fraudulent activity, including acts of ML/FT, as determined at the company's sole discretion is strictly prohibited. Fraudulent activity may include, but is not limited to:

- Stolen funding methods
- Forgery of documentation;
- Collusion (for which such is not possible at the current stage of operation);
- The use of impermissible software tools to render the Client anonymous;
- The provision of false registration data or other requested information;
- Any red flag identified above.
- Any act of manipulation and deceit

Clients where there is suspicion, knowledge or reasonable grounds to suspect that they are involved in fraudulent activity, ML or FT will be reported to the appropriate authorities within the stipulated time frame, which is **IMMEDIATELY UPON THE SUSPICION BEING RAISED** via the Suspicious Activity Report Form. All personnel have direct access to the MLRO or Deputy MLRO, and such reports should be raised immediately. Once an STR/SAR has been escalated, it will be included in a STR/SAR central repository within the organisation. The company shall at all times retain any STR/SAR as follows:

- Reports raised to the FIU;
- Reports not raised also hold information on why the report was not raised.

The company may occasionally receive requests for information or notifications from regulatory authorities or law enforcement bodies regarding investigations of a criminal, civil or regulatory nature. When such requests for information are received, these are to be forwarded in their entirety to the company MLRO. The company MLRO or deputy MLRO will handle and process these requests in line with the following process; the appointed officer will:

- Record the receipt of such a request;
- Verify the legitimacy of the requesting organisation and individual making this request;
- Verify the legal basis under which such a request is made;
- Identify the customer (or customers) accounts relevant to the request;
- Analyse the customer's information, including, amongst others, due diligence, transactions and ongoing monitoring information;
- Re-consider the customer's risk status considering the received request and take appropriate action depending on the case;

- Identify information that is relevant to the request and following a due assessment of the information, prepare and provide the information to the requestor; and
- Update the company records in respect of such a request and where appropriate, notify the relevant regulators or authorities with follow-up actions as per relevant regulatory obligations.

Reporting of suspicious activity or transactions and requests for information shall be done via the GOAML system by the MLRO or Deputy MLRO acting in the absence of the MLRO.

The authorities will review the suspicion on information provided and send an acknowledgement within 24 hours. If more information is required, the MLRO will request it from the contacting staff. In this time, transactions are not to be carried out without the consent of the MLRO. If the MLRO gives consent to proceed with a transaction, then that consent only applies to that specific transaction. If the Client requests further activities or transactions, further consent is required from the MLRO. Unless instruction has been given to terminate the business relationship.

No one is to divulge to co-workers, line managers and especially the customer/s that an STR/SAR has been raised as this is potentially considered to be 'tipping-off'. Tipping-off is a criminal offence and an individual found guilty of a tipping-off offence may be held personally liable.

37. Thresholds Limits and Controls

The company shall be able to place thresholds in relation to SOW/F information identified or verified. This shall be common practice to ensure that the Client's trade is within their set profile, and if exceeded, the Client shall be questioned regarding the source of funds of said transaction. This is intended to prevent Clients from trading beyond their means, and shall also serve as a means where the company can easily detect any illicit activity occurring and/or which may occur.

In such a case, the Client will be prompted to provide the source of funds for the transactions, and a re-evaluation of the Client's profile will be conducted. The client may be given an extension if deemed to be high net worth, funds are fully verified, and at a discretionary basis the threshold may be increased upon approval of the MLRO or the Deputy in his absence, such shall be substantiated the an understanding of the client, the affordability, and the case in general.

The company has adopted a procedure of reviewing and ranking the jurisdictions involved in the company's operations at a minimum annually. The jurisdiction list is compiled via several sources (see the list of sources below). An exhaustive assessment is carried out, and an internal scoring is assigned accordingly; such risk level will be then reflected as part of the CRA.

The development and implementation of appropriate measures and procedures on a risk-based approach, and for the implementation of Client Identification and Verification and Due Diligence Procedures, the MLRO and the Compliance Officer shall consult data, information and reports [e.g. Clients from countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), country assessment reports] that are published in the following relevant international organisations in order to determine the geographical risk posed by a Client:

- FATF - www.fatf-gafi.org
- Business and sanctions consulting <https://www.bscn.nl/sanctions-consulting/sanctions-list-countries>
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money
- Laundering Measures (hereinafter "MONEYVAL") - www.coe.int/moneyval
- The EU Common Foreign & Security Policy (CFSP)-
- http://ec.europa.eu/external_relations/cfsp/sanctions/list/consol-list.htm
- The UN Security Council Sanctions Committees - www.un.org/sc/committees
- The International Money Laundering Information Network (IMOLIN) -
- https://www.imolin.org/imolin/amlid/index.jsp?lf_id=
- The International Monetary Fund (IMF) – www.imf.org
- The Office of Foreign Assets Control (OFAC) of the US Department of the Treasury -
- <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx>
- FIU website
- Basel international jurisdiction list.

Black listed countries
Iran , North Korea, Myanmar
Countries where online gambling for citizens is banned
United Arab Emirates, Brunei, Cambodia, North Korea, Japan, Singapore, Cyprus, and Qatar.
Banned Foreign Gaming Sites
Georgia, Sri Lanka, Austria, Belgium, Bulgaria, Croatia, Denmark, Estonia, Finland, France, Germany, Italy, Poland, Romania, Spain, UK, USA and Panama.
FATF Greylisted countries
Bulgaria, Burkina Faso, Cameroon, Democratic Republic of the Congo, Croatia, Haiti, Jamaica, Kenya, Mali, Mozambique, Namibia, Nigeria, Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Türkiye, Vietnam, Yemen
Curacao treaties and prohibitions
USA, the Netherlands, France, Dutch West Indies, and Australia.

39.

Policy, Compliance and Review

Compliance will be continually monitored through any or all of the following methods:

- File audits;
- Review of records maintained;
- Reports or feedback from staff; and

Sunrise Worldwide Solution N.V

- Any other method.

We will review this policy at least annually as part of our overall risk management process. We will also review this policy if:

- There are any major changes in the law or practice;
- We identify or are alerted to a weakness in the policy; or
- There are changes in our business, our Clients or other changes which impact this policy.

The company takes compliance with this policy very seriously as failing to comply puts the staff and the company at risk. We may commit a criminal offence if staff fail to comply with this policy and the AML and CFT regimes carry heavy criminal penalties according to the local jurisdictions. If any aspect of this policy, or any of the related procedures, are breached, the incident must immediately be reported to the MLRO. Due to the importance of this policy, a failure to comply with any requirement may lead to disciplinary action, which may result in dismissal.

To ensure compliance management the following has been implemented as follows:

- Client file reviews are to be conducted at a minimum twice a year to ensure quality and assurance testing
- A review as indicated above shall be carried out to ensure that all policies are held up to date and are reflective of the current methodology
- External audits are to be conducted annually
- Spot checks are to be carried out and proactive investigations are to be carried out on subsets of clients as set by the MLRO.

30. Conclusion

The above are the company's policies AML and CTF, as well as the information required in relation to our KYC services. This policy will change according to the company's business practices and will be updated accordingly

Sunrise Worldwide Solution N.V

Sunrise Worldwide Solution N.V