

Anti-Money Laundering & Combating of Terrorism Finance *Company Manual*

IT MANAGEMENT SANTORA B.V.

Table of Contents

Abbreviations.....	4
About this manual	6
Part One – IT Management Santora B.V.’s compliance ethos	6
1.0 Prevention of criminal activity, money laundering and funding of terrorism	6
2.0 Compliance Culture	6
2.1 Vision.....	6
2.2 Compliance	6
2.3 Quality	7
3.0 General.....	8
3.1 Application of the manual.....	8
3.2 Definition of money laundering and facts/stages.....	8
3.3 Employee Access to the manual	9
4.0 Compliance Officer	9
4.1 Duties of the Compliance Officer.....	9
5.0 Application of Appropriate Measures and Procedures on A Risk Based Approach.....	10
5.1 General policy	10
5.2 Identification of risks	11
5.3 Design and implementation of measures and procedures to manage and mitigate the risks	14
6.0 Client Acceptance Policy (CAP)	15
6.1 Assessing Player Behaviour	19
6.2 Player Name Screening & Sanctions Screening Procedures.....	21
6.3 The Risk Assessment	22
6.3.1 Customer Risk Scoring	23
6.3.2 Channel Risk Scoring	23
6.3.3 Funding Risk Scoring	24
6.3.4 Product or Service Risk Scoring	24
6.3.5 Geographical Risk Scoring	25
6.3.6 Other Risk Scoring.....	27
6.3.7 High Risk Source of Funds	27
6.4 Residency of Players allowed to use IT Management Santora B.V.’s services.....	28
7.0 Client Due Diligence and Identification Procedures	30
7.1 Due Diligence Procedures on Natural Persons (Players)	30
7.2 Non face to face meetings	32
7.3 Politically Exposed Persons – PEP’s.....	32

7.4 Reliance on other subject persons or third parties	33
8.0 Information on the purposes and intended nature of the business relationship.....	35
8.1 Personal Details of the player.....	35
8.2 Source of Wealth and Source of Funds	36
8.3 Expected Future Deposits	37
8.4 Player Declarations.....	37
9.0 Ongoing Monitoring Process.....	39
9.0.1 Updating missing due diligence of Players	40
9.1 Timing of CDD procedures.....	40
9.1.1 Analysing the Naf 4,000 and Naf 5,000 Thresholds	41
9.2 Simplified Due Diligence.....	41
9.3 Customer Due Diligence & The Know Your Customer (KYC) Process	42
9.4 Enhanced Due Diligence.....	42
10.0 Recognition and reporting of suspicious transactions/activities	44
10.1 Internal reporting procedures.....	44
10.1.1 Examples of situations which may lead to the filing of an UTR.....	44
10.2 External reporting procedures	45
10.3 Obligation to refrain from carrying out a transaction that appears to be suspicious	46
10.4 Dealing with non-cooperative players.....	46
11.0 Record-keeping procedures.....	47
12.0 Education.....	48
12.1 Employees' education and training policy	48
12.1.1 Minimum content of AML Training	49
12.2 Vetting of new employees	49
13.0 Approval and updating of AML Manual	51
14.0 Contact Information.....	51
Appendix A – Internal UTR Form.....	52
References	55

Manual Version	Drafted / Updated by	Approved By	Approval Date
V1.0	John Caruana / A2CO		
V1.1	Gabriela Xuereb / Compliance Officer		

Definitions

In this manual, except where it follows otherwise from the context:

“Players” – In the context of IT Management Santora B.V. (“IT Management Santora”), a player is a person registered with the license holder.

“Business relationship” means a business, professional or commercial relationship which is connected with the professional activities of IT Management Santora B.V. and which was expected, at the time when the contact was established, to have an element of duration.

“Occasional transaction” means any transaction other than a transaction carried out in the exercise of an established business relationship formed by a person acting either in the course of relevant financial business or in the course of relevant activity.

“Politically exposed persons” means natural persons who are, or have been, entrusted with prominent public functions and shall include their immediate family members or persons known to be close associates of such persons, but shall not include middle ranking or more junior officials. This shall also apply to local politically exposed persons. A detailed definition shall be provided within this manual.

Abbreviations

AML/CFT	Anti-Money Laundering / Combating Financing of Terrorism
CDD	Customer Due Diligence
EDD	Enhanced Customer Due Diligence
LBP	Landsverordening Bescherming Persoonsgegevens (National Ordinance On The Protection of Personal Data)
ML/FT	Money Laundering and Financing of Terrorism
CO	Compliance Officer (equivalent to MLRO)
CGA	Curaçao Gaming Authority
MONEYVAL	The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
PEP	Politically Exposed Person
LID	Landsverordening Identificatie bij Dienstverlening (National Ordinance on Identification when Rendering Services)
LMOT	Landsverordening Melding Ongebruikelijke Transacties (National Ordinance On The Reporting of Unusual Transactions)
LOK	Landsverordening op de kansspelen (National Ordinance on Games of Chance)
SW	Rijkssanctiewet (Kingdom Sanctions Law)
SNO	Sanctielandsverordening (Sanctions National Ordinance)
SDD	Simplified Customer Due Diligence
UTR	Unusual Transaction Report

Updates Made to Manual V 1.0 – May 2025

- The AML Policy has been revamped in its entirety, with comprehensive updates made across all sections to align the Manual with the latest Curaçao AML/CFT/CPF regulatory framework, FIU Curaçao guidance, and Gaming Control Board (GCB) Regulations (January 2025).

Updates Made to Manual V 1.1 – February 2026

- Updated Wording and Abbreviations to align with recent amendments and terminology adopted by Curaçao authorities.
- Updated Compliance Officer email address throughout the Manual to reflect the new official email address for submitting Unusual Transaction Reports (UTRs) to the FIU Curaçao
- Updated Section 6.0 Client Acceptance Policy to include paragraph to address Level 3 procedures, which shall apply when a player reaches the Naf 5,000 threshold in one gaming day.
- Updated Section 6.2.1 Screening Process and Scope, 6.2.2. Review and Escalation, 6.2.4 Ongoing Monitoring and Record-Keeping to streamline and clarify the procedures
- Updated Section 6.2.3. Sanctions & Proliferation Financing Controls.
- Updated Section 6.3.5. FATF and EU List of Countries to align with the most recent FATF and EU publications.
- Updated Section 7.4 Reliance on other subject persons or third parties to align with regulatory expectations.
- Added new Section 14.0 to include contact information, providing key contact details for regulatory and reporting purposes.
- Updated Section 12.1 Employees Education and Training Policy to update list of regulatory frameworks and guidance documents, ensuring employee awareness aligns with the most recent Curaçao AML/CFT and sanctions obligations.
- Revised Section 12.3 Ongoing Testing of Outsourcing Providers to ensure it reflects current information
- Added new references to the Reference List

About this manual

This manual is intended to put in writing any policies or procedures that IT Management Santora B.V. applies within their day-to-day duties as a Gaming Company licensed by the Curacao Gaming Authority. All employees of IT Management Santora B.V. shall review and agree with this manual upon employment and at least once annually.

Part One – IT Management Santora B.V.’s compliance ethos

1.0 Prevention of criminal activity, money laundering and funding of terrorism

IT Management Santora B.V.’s future success depends, inter alia, upon the maintenance of the firm’s reputation of probity. It is therefore vital that we avoid exposure to, and involvement in, relationships concerning the proceeds of crime; terrorism financing; and accordingly, money laundering.

Evidence of potential money laundering activity often occurs in the form of unusual or unexpected patterns of transactional activity, including through betting. Adherence to satisfactory AML/CFT procedures provides the foundation for the recognition of such activity. Adequate customer due diligence should enable us to know enough about our players such that we can recognise unusual or unexpected activity when, or before, it occurs, in addition to helping us to identify and manage the risks inherent in business relationships.

2.0 Compliance Culture

2.1 Vision

To provide high quality and efficient gaming services while ensuring to be in line with any AML/CFT regulations.

2.2 Compliance

Since IT Management Santora B.V. is licensed as a Business-to-Consumer (B2C) operator, in addition to its Business-to-Business (B2B) activities, it is deemed a subject person under Curaçaoan law. As such, it is required to implement appropriate processes and controls in line with the obligations set out under the National Ordinance on Games of Chance (LOK), the National Ordinance on Identification when Rendering Services (LID), the National Ordinance on the Reporting of Unusual Transactions (LMOT), the Sanctions National Ordinance (Sanctielandsverordening), the Kingdom Sanctions Act (Rijkssanctiewet), as well as any other applicable regulatory requirements as may be in force from time to time. This manual sets out the minimum mandatory requirements by which IT Management Santora B.V. and each staff member must adhere to.

Notwithstanding that IT Management Santora B.V. strives to be, and remain, a profitable business, the highest priority must be given to establishing and maintaining an effective compliance regime and

culture. Compliance (including the prevention of criminal activity, money laundering and funding of terrorism) is a core value and fundamental to the society we now inhabit. A positive approach to compliance must influence all we do. We must approach our players and our work in the spirit of compliance.

Adherence to this manual is considered of utmost importance. Compliance with the requirements set out in this document is therefore mandatory.

2.3 Quality

Our quality policy encompasses:

- A commitment to meet the requirements of this manual and prevailing supervisory and AML laws, regulations and guidelines, issued by the authorities in Curacao;
- Commitment to continually improve and tighten our procedures and strive for excellence in all we do;
- A commitment to continually review our quality policy and update this manual to reflect changes in relevant legislation;
- It is the responsibility of the Compliance Officer to monitor compliance with the objectives and spirit of this manual.
- It is the responsibility of the Board of Directors to ensure that all resources are provided to the company, its employees and the Compliance Officer to ensure that the policies and procedures written in this manual are applied and followed.

Part Two: Rules applicable

3.0 General

IT Management Santora B.V. has put in place several procedural AML/CFT checks and practices in line with the Law, which are laid out in this manual, and which must be applied by the Gaming Company itself and any employees who are involved in the provision of relevant activities as defined by the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction.

This manual has been developed, and will be periodically updated, by **Gabriela Xuereb** santora@a2co.com as the Compliance Officer in relation to the prevention of money laundering and terrorist financing, for Curacao Gaming License, in Curacao.

The manual's aim is to prevent money laundering and terrorism financing, in accordance with the risk profile of our products, services, customers and geographic locations.

3.1 Application of the manual

Compliance with this Manual by the Compliance Officer and all employees is mandatory. Failure to follow the procedures described in this manual may result in disciplinary action, including possible termination.

The Compliance Officer must ensure that this manual is adequately implemented and periodically monitored and tested. The Board of Directors shall ensure that the required access and resources are provided to the Compliance Officer to enable her to perform her duties.

3.2 Definition of money laundering and facts/stages

Money laundering takes place when funds acquired from illegal activities (e.g. theft, drug trafficking, prostitution, tax evasion) are circulated in ways that withhold their origin. The main objective of money laundering is that monies acquired in illicit activities pass through various hands and systems, so that it is no longer possible to trace the source of those funds.

Funding of terrorism takes place when funds acquired from activities that may be legal (e.g. raised as charity from people who thought they were donating towards a just cause) as well as illegal are circulated in ways so as to withhold both their origin and destination. The destination of the funds is the planned act of terrorism for which the funds were planned. Such funds would be utilised in various ways, including training camps for terrorists, dealing in weapons, and so on.

Money laundering and funding of terrorism normally takes place in the following ways:

- Transfers of funds from a financial institution (e.g. a bank) to another, or from one account to another, or from one country to another;
- Deposits of funds in a financial institution in a country guaranteeing anonymity and/or not having strong legislation against money laundering;

- Acquisition of property, vehicles, vessels, and other assets in cash, and possibly in other peoples' names, which are then re-sold;
- Casino gambling, by way of buying large amounts of chips, and then re-cashing them from the casino;
- Remote gaming, by depositing funds which are derived from illegal activities and then withdrawing them, transferring them to third parties, or perform collusion through games of skill such as Poker;
- Always being represented by an agent or intermediary, trying to hide one's own identity.

Thus, due to the nature of the business of IT Management Santora B.V. the main exposure for ML/FT is through the variation of gaming products, some of which may be inherently riskier and can be more attractive to criminals. Specific funding methods are also treated as high risk factors for ML/FT including anonymous payment methods that may interrupt the audit trail.

3.3 Employee Access to the manual

It is also important to highlight that the AML Manual will be shared with all employees by email, making sure everyone has direct access to the most up-to-date version. This approach also ensures that any updates or changes to the Manual are quickly communicated to all staff. As part of the Company's ongoing commitment to building a strong culture of compliance, new employees will receive access to the AML Manual during their onboarding. This helps them understand their responsibilities, the Company's policies and procedures, and what is expected of them right from the start of their employment.

4.0 Compliance Officer

4.1 Duties of the Compliance Officer

The duties of the Compliance Officer shall include, inter alia, the following:

- Development of and adherence to the business's anti-money laundering procedures;
- To review players flagged by the Risk Management or Compliance teams which resulted in abnormal behaviour or had a possible hit in the name screening procedure performed by the team;
- Perform an overview and monitoring of customers who reached the NAF 4,000 deposit (this threshold is subject to change based on currency fluctuations; however, at the time of drafting this manual, it is equivalent to approximately EUR 2,000) after being notified by the respective team on such players;
- Perform frequent tests to ensure that proper due diligence procedures are being implemented by the respective teams (such as Risk Management / Compliance);
- Provide to the Board of Directors a report on a regular basis on such testing and/or any other AML related matters;
- The provision of adequate training to relevant employees and to keep up to date with training herself. Such training to employees may also be outsourced if deemed necessary by the Compliance Officer or the Board;

- Ensure that the business has a clear policy in place when a suspicion on a transaction or customer in relation to ML/FT arises;
- Collate reports received, consider their contents and report those deemed suspicious to the FIU Curaçao via the GoAML secured system. The Compliance Officer needs to keep records of all those internal UTRs on which it was decided that an UTR to the FIU Curaçao is not filed and the reasons behind such decisions;
- Ensure that all records are securely maintained; and
- Ensure policies and procedures are kept updated and effective.

5.0 Application of Appropriate Measures and Procedures on A Risk Based Approach

5.1 General policy

IT Management Santora B.V. shall apply the appropriate measures and procedures, including use of the CDD, by adopting a risk-based approach, so as to focus its effort in those areas where the risk of money laundering and terrorist financing appears to be comparatively higher. Due to the nature of the business, such implementation shall be affected in practice through the assistance of various teams, including the Risk Management Team and Compliance Team. The scope of having a risk-based approach is to avoid focusing resources where there is lower risk of ML/FT, while focusing more resources where high level of risk is identified.

Furthermore, the Compliance Officer, shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures. Such testing of effectiveness of the measures applied may be outsourced to third party industry professionals which may provide the company with a report on the level of effectiveness. However, the responsibility to ensure that such effectiveness is in place on an ongoing basis lies with the Board of Directors of the Company. The adopted risk-based approach that is followed by IT Management Santora B.V. and described in the manual, has the following general characteristics:

- Recognises that the money laundering or terrorist financing threat varies across clients, countries, products / services and the channels used to establish a business relationship;
- Allows the business to apply its own approach in the formulation of policies, procedures and controls in response to particular circumstances and characteristics;
- Helps to produce a more cost-effective system; and
- Promotes the prioritisation of effort and actions of the business in response to the likelihood of money laundering and terrorist financing occurring using its services.

The risk-based approach adopted by IT Management Santora B.V., and described in the manual, involves specific measures and procedures in assessing the most cost-effective and appropriate way to identify and manage the money laundering and terrorist financing risks faced by the business.

Such measures include:

- Identifying and assessing the money laundering and terrorist financing risks emanating from particular players, type of gaming products (games), client interface, the jurisdiction of residence of the players, their nationality together with any other jurisdictions in which players

have a vested interest, transaction risk, and whether the player is exposed to other high-risk factors as established within the risk model.

- Managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls; and
- Continuous monitoring and improvements in the effective operation of the policies, procedures and controls.

The application of appropriate measures and the nature and extent of the procedures on a risk-based approach depends on different indicators. Such indicators include the following:

- Scale and complexity of the betting products offered;
- Geographical spread of the services and players;
- Nature (e.g. non-face-to-face) and economic profile of players;
- Distribution channels and practices of providing services;
- Volume and size of transactions / deposits;
- Degree of risk associated with each type of gaming service;
- Country of origin and destination of clients' funds;
- Deviations from the anticipated level of transactions; and
- Nature of business transactions.

The Compliance Officer shall be responsible for the development of the policies, procedures and controls in the CDD on a risk-based approach. Furthermore, the Compliance Officer shall also be responsible for the implementation of the policies, procedures and controls on a risk-based approach. The Compliance Officer shall monitor that an updated version of this manual, due diligence of players, ongoing due diligence, and risk analysis of players are kept up to date. Furthermore, the Compliance Officer is to ensure staff are well trained on AML/CFT and on these policies and procedures.

5.2 Identification of risks

The risk-based approach of the CDD adopted by IT Management Santora B.V. involves the identification, recording and evaluation of the risks that have to be managed. The CDD includes the client due diligence systems and procedures of IT Management Santora B.V. and is used during the implementation of the client acceptance policy and ongoing monitoring, including an annual review of clients where high risk is noted.

IT Management Santora B.V. shall assess and evaluate the risks the business faces for the use of their Gaming services for the purpose of money laundering and terrorist financing. IT Management Santora B.V. shall be, at all times, in a position to demonstrate to the relevant authorities that the extent of measures and control procedures it applies (whether in the CDD or otherwise) are proportionate to the risk it faces for the use of its services for the purpose of money laundering and terrorist financing.

A more detailed and separate document on the risks of the business has been drafted. This report shall be kept up to date with at least an annual update. The document shall be referred to as the 'Business Risk Assessment' and includes the identification of all risks, how these are being mitigated and their likelihood of taking place. The Business Risk Assessment report can be made available to competent authorities upon request.

Since IT Management Santora B.V. is a licensed gaming company (B2C) under the Curacao Gaming Authority, it falls under the remit of the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, as well as other applicable laws, which already have been referenced above. The risk assessment on players shall be carried out when the total deposit from such player is equal to or above NAf 4,000. The regulation does not specify a timeframe, meaning that this threshold applies over the player's lifetime.

5.2.1 Business risks

The following, inter alia, are sources of risks which IT Management Santora B.V. faces with respect to money laundering and terrorism financing, and which must be taken into account in assessing the risk posed by a particular player and/or business relationship. The final risk assessment will be case-specific, taking into account a holistic view of the risks posed by the player and the specific circumstances of the business relationship, as well as the high-risk categories as prescribed at law, which require the application of EDD measures (see further Section 9.4 of this manual on EDD measures). The following risks are being captured by the risk model. A more detailed information about the risks of IT Management Santora B.V. business may be found in the 'Business Risk Assessment' report.

(a) Customer risk - risks based on the client's nature:

Below is a non-exhaustive list of customers whose activities may pose a higher risk:

- a. Whether the player is a Politically Exposed Person (PEP);
- b. Whether the player is a Sanctioned individual;
- c. Whether the player is mentioned in adverse media;
- d. Whether this is a doubt about the authenticity of the documents provided;
- e. Whether the source of wealth is related to high risk sources;
- f. Whether the player benefitted or is a prospective applicant of citizenship or residency by investment schemes;
- g. Whether the player was reluctant to provide due diligence documentation;
- h. Whether the player has a multiple source of income.

(b) Channel Risk - the channels through which a business relationship is established and through which transactions are carried out:

- Non-face-to-face clients;
- Non-face-to-face using digital ID&V and Biometric Verification (Sumsu)

Due to the nature of the business, face-to-face relationships are not expected. In fact, the company expects all customers to be considered as non-face-to-face, however, it is currently investing in technology, specifically by utilising Sumsu, an AI-powered identification tool, to mitigate against the risks related to such pillar.

(c) Funding Method Risk

- The company accepts payments via e-wallets (Skrill, Neteller, MuchBetter) and direct bank transfer (Instadebit)
- Cash payments are not acceptable.
- Payments by cheques are not acceptable.
- Payment by anonymous sources are not acceptable.
- The payment shall be from a source in the name of the player. Transfers between players are also not allowed by the company.

(d) Product risk - some gaming products are inherently riskier than others and are therefore more attractive to criminals. The company offers multiple types of gaming products, namely casino games (including, slots, roulette); live casino games (including, blackjack, roulette, baccarat, poker); sportsbook (including football, basketball, tennis, American football, ice hockey); virtual sports (virtual football, virtual cycling, virtual horse riding, virtual greyhounds, virtual drag racing, and virtual tennis); esports games (including; counter strike, call of duty, starcraft, halo, e-football and e-basketball). In and of itself, Poker and Peer-to-Peer Gaming present a higher risk due to the possibility of collusion between the players.

- Client making a typical use of the service being provided;
- Transactions to and from unknown sources;
- Reportable transaction activity;
- Unexplained activity which is not aligned to expectations; and
- Services that inherently provide more anonymity or can readily cross international borders, such as private investment companies and trusts;

(e) Jurisdiction risk - the risk posed by the geographical location of the business/economic activity and the source of wealth/funds of the business:

- Players from high-risk countries or countries known for high-level of corruption or organised crime or drug trafficking;
- Countries on the FATF list of high-risk jurisdictions subject to a Call for Action;
- Countries on the FATF list of jurisdictions under Increased Monitoring;
- Countries subject to sanctions, embargoes or similar measures issued by international organisations including OFAC, UN, EU;
- Countries on the CFATF Public Statement;
- Countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's Annual International Narcotics Control Strategy Report (INCSR);
- Countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime;
- Countries identified by credible sources as providing funding or support for terrorism activities or that have designated terrorist organisations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International;

Specifically, in relation to geographical risk, IT Management Santora B.V. carries out country risk assessments with respect to jurisdictions from which the player lives or jurisdictions which are somehow linked to the wealth generation of the player.

For the purpose of determining whether a jurisdiction is reputable or otherwise, the Compliance Officer shall consider reports and other publications issued by the FATF, the European Commission, IMF, World Bank and Transparency International, amongst others. The Compliance Officer will review the jurisdictional assessment from time to time in line with developments.

IT Management Santora B.V. also takes into account national and supranational risks by taking into consideration several reports on jurisdictions which are available to the public when assessing such a risk.

(f) Other Risks

Players may expose the company to other types of ML/FT risks which are considered as 'high'. In fact, these risks mentioned below are loaded with a scoring which would override the player to an overall risk classification to 'High', hence triggering EDD. These are the following scenarios:

- Attempt to use fake documentation;
- Attempt to open multiple accounts from the same location;
- Abnormal betting patterns identified;
- Abnormal Deposits or withdrawals patterns;
- Attempted deposit/payment by a third party on behalf of a player.

5.3 Design and implementation of measures and procedures to manage and mitigate the risks

Taking into consideration the assessed risks, the Gaming Company shall determine the type and extent of measures it will adopt to manage and mitigate the identified risks in a cost-effective manner. These measures and procedures include:

- a) Adoption of the client due diligence procedures in respect of players in line with their assessed money laundering and terrorist financing risk, following meeting of the NAf 4,000 deposits;
- b) Requirement for the quality and extent of identification of data for each type of client to be of a certain standard (e.g. documents from independent and reliable sources, third-person information, and documentary evidence, where possible. One should note that player identity verification procedures will take place within a 30-day period from the moment the NAf 4,000 are placed;
- c) Obtaining additional data and information from the player, where this is appropriate and applicable for the proper and complete understanding of their activities and source of wealth, and for the effective management of any increased risk emanating from the particular business relationship or the occasional transaction. This is performed for high-risk players following the NAf 4,000 or before if there is a suspicion of ML/FT;

d) Ongoing monitoring of player transactions and activities from the initialisation of the business relationship to ensure that:

- ➔ The player is not using multiple accounts from the same IP Address in order to avoid the CDD threshold;
- ➔ The player is not using fake identification details;
- ➔ The player is not indicating abnormal betting patterns;
- ➔ The player is not indicating abnormal deposit or withdrawal patterns or activities;
- ➔ The player is not playing from an IP/Geo Location which differs from the declared country of residency;
- ➔ The player is not showing any abnormalities or suspicious behaviour during his or her usage of our services; and
- ➔ The player's identification documents are not expired.

Should there be a suspicion or knowledge of ML/FT, then please refer to section 10.1 for the internal reporting procedures of the company.

Whether or not to accept a player will depend on the risk factors outlined in Section 5.2.1 above and on other factors such as whether the NAf 4,000 threshold is reached and name screening results. Once these risk elements are considered thoroughly, a decision has to be taken whether to accept the client or not in accordance with the client acceptance policy outlined in Section 6 below.

If a player is considered to present a high risk of ML/FT, the player could be accepted under higher monitoring or refused. Players who are considered to pose a 'high-risk' must be subject to enhanced due diligence procedures if such players have exceeded the NAf 4,000 threshold.

6.0 Client Acceptance Policy (CAP)

The client acceptance policy defines the criteria for accepting new clients (players) and defines the client categorisation criteria which shall be followed by IT Management Santora B.V.

The company shall onboard players on two levels:

Level 0: Unregistered Players

Unregistered Players will not be able to place any stakes on the websites owned by IT Management Santora B.V. Therefore, an individual cannot participate in a game for money unless that individual is an Account Holder. To be registered as a player, an individual must register personally and submit an application for registration.

Level 1: Before NAf 4,000

At this level, the company shall ask the player to provide at least the information listed in section 8.1 Personal Details of the player. In case of funding emanating through deposits, the system shall also not allow players to wager if the verification of the player's control over the wallet.

The company will then monitor the transactions of the player and his or her behaviour such as changes in the betting behaviour, deposit behaviour, changes in funding methods and games being played. Furthermore, the company shall monitor the total deposits of the player (excluding bonuses and winnings) and ensure the total deposit does not meet the NAf 4,000 as established by the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction. The total deposit threshold shall be calculated across all platforms the company is offering under its Curacao Gaming License. If the threshold is met, then Level 2 of the onboarding will be initiated as noted below.

Level 2 – After NAf 4,000 is reached

Once the NAf 4,000 threshold is reached by the player; the company shall initiate the following procedure:

- a. The account of the player is blocked from the ability to make withdrawals as the player is provided 30 days to provide the requested information.
- b. The compliance team shall provide the player with a set of due diligence questions which shall include:
 - Additional personal details including the nationality, place of birth, countries having vested interest in, and whether the player has any additional citizenships.
 - Details about the source of wealth and the income of the player. This includes the source of how the wealth was accumulated, the employment situation of the player, the current occupation, the annual income of the player and whether this is derived from a single or multiple source. Furthermore, an estimate of the overall net worth of the player is asked to be provided through the selection of specific categories. Further information on the wealth is obtained by requesting the types of assets forming such wealth. The player is also asked to provide whether his wealth is derived from certain high-risk sources such as cash intensive activities, arms trade, defense or mining activities or cryptocurrencies.
 - The player is also asked to provide the expected amounts he or she is expecting to deposit with the company on a monthly basis.
 - The player is asked to confirm whether he/she or the immediate family members is/are considered as Politically Exposed Persons. The definition of a PEP under the Curaçaoan regulations is to be provided.
 - Furthermore, the player is requested to confirm a set of declarations to ensure he or she is of good repute and to ensure the player confirms the information provided is full, correct, and complete.
 - The player is to confirm that he or she is not representing a third party.
- c. The Client Risk Assessment (CRA) as noted in section 6.3 is performed to assess the risk classification of the customer based on the information provided as noted in 'b' above.

- d. If the CRA classifies the customer (player) as 'high risk', then the compliance team shall initiate Enhanced Due Diligence procedures as noted in section 9.4. This will also require supporting wealth documentation from the player.
- e. If the player does not provide the due diligence requested within a 30-day period, the company shall suspend and terminate the player from its platform. The company shall return the funds on account to the customer's bank account, ideally through the same channels such funds were received, if possible, unless there are suspicions or knowledge of ML/FT.
- f. Point 'e' above shall not take place if there is suspicion of ML/FT. In such a situation an internal UTR should be submitted in line with procedures defined in section 10.1. In such situations, the Compliance Officer shall provide the clearance of such money on account to be transferred to the player.
- g. Terminated customers shall not be re-onboarded unless approved by the Compliance Officer.
- h. Further to the above, once the player who reached the Naf 4,000 provides the onboarding questionnaire, the following procedure is to be followed:
 - The Risk Management or Compliance Team shall ensure that the questionnaire is completed;
 - The Risk Management or Compliance Team shall ensure that the questionnaire is translated to English, and such translation is kept on file;
 - The following documents are to be sent to the Compliance Officer for her feedback:
 - a) The original questionnaire as received from the player
 - b) The translated questionnaire (if applicable or required)
 - c) The risk classification of the player
 - d) Any wealth supporting documentation provided by the player
 - The Compliance Officer shall provide feedback to the Risk Management team
 - The Risk Management Team shall then liaise with the Customer Support Team, who will contact the player to obtain any additional information as recommended by the Compliance Officer. Any updated documentation shall be provided to the Compliance Officer once received.
 - If the said documentation is not received by the player, the Risk Management team shall inform the Compliance Officer accordingly;
 - It is being highlighted that the player's account shall remain blocked until otherwise instructed by the Compliance Officer.

The client acceptance process involves:

- All staff must be aware of the business's policies and procedures especially with regards to the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction;
- Before accepting or continuing servicing a client, the compliance team shall obtain the necessary due diligence to enable them to assess the client and engagement within the 2nd

level of onboarding as noted above and basic identification information as noted in the 1st level of onboarding;

- The company must also obtain information on the nature of services to be provided – which by nature is known since the service will always be related to the provision of gaming services, however, the expected type of gaming services to be used by the account, is to be provided by the player.
- Where necessary, the compliance team or the Compliance Officer shall enquire on the client's bankers, legal advisors and any other business relationships;
- The documentation gathered will be documented within the customer's file;
- Once the Naf 4,000 threshold is reached, the engagement will be terminated if the full due diligence documentation in line with Enhanced Due Diligence procedures as noted in section 9.4, is not received within 30 days;
- IT Management Santora B.V. shall perform EDD when the client is classified as high-risk through the CRA after the Naf 4,000 threshold is met or if there is suspicion of ML/FT at any time;
- The company uses the following risk indicators when onboarding a client:
 - (b) Customer risk
 - (c) Product/Service risk
 - (d) Interface risk (Channel Risk)
 - (e) Geographical risk
 - (f) Transaction Risk
 - (g) Complexity of the Structure
 - (h) National and/or Supranational Risks (if any)

IT Management Santora B.V. shall classify clients into 3 categories:

1. Low-risk clients,
2. Medium-risk clients, or
3. High-risk clients

Level 3 – After Naf 5,000 is reached in one gaming day

In line with NORUT, IT Management Santora B.V. is required to treat any transaction that equals or exceeds Naf 5,000 (or the foreign currency equivalent) in a single gaming day as an unusual transaction. Once this threshold is reached, the transaction must be documented and reported to the FIU through the goAML portal, in accordance with applicable legislation and FIU reporting guidelines.

The Naf 5,000 threshold applies to both single transactions and series of linked transactions that, when aggregated, meet or exceed this amount within a single gaming day. It applies irrespective of the payment method, including but not limited to:

- Cash transactions
- Cheques or other negotiable instruments
- Electronic or digital payments, including e-wallets and credit cards
- Chip, token, or credit purchases
- Deposits or withdrawals made at the request of the player
- Bank transfers, whether local or international

The following are typical examples of transactions that trigger the reporting obligation:

- Cashless transactions (e.g., bank transfers) of NAf 5,000 or more at the player's request.
- Accepting or releasing deposits of NAf 5,000 or more.
- Sales of chips, tokens, or credits totalling NAf 5,000 or more.
- Cash-outs of NAf 5,000 or more.
- Structuring or splitting transactions to cumulatively exceed NAf 5,000 within a gaming day.

Once the NAf 5,000 threshold is reached or exceeded in one gaming day, the following procedure shall be followed:

a) Internal Escalation

The employee identifying the transaction must immediately inform the Compliance Officer, providing full details and any supporting documentation.

b) Review by Compliance Officer

The Compliance Officer shall review the transaction to confirm that the NAf 5,000 objective indicator has been triggered and ensure all required information is collected.

c) Timely Reporting to FIU

The Compliance Officer must submit the report to the FIU via the goAML portal without delay, and in any case within the legal reporting timeframe applicable to objective indicators. Reports must be submitted in English and include all relevant supporting documentation.

d) Record Keeping

All documentation related to transactions meeting or exceeding the NAf 5,000 threshold—including the rationale for reporting or non-reporting—must be retained for at least five years, in line with Curaçao's record-keeping requirements.

All employees must maintain strict confidentiality regarding the identification and reporting of transactions that meet the NAf 5,000 threshold. No information about the report may be disclosed to the customer or third parties, in accordance with NORUT. Any disclosure could constitute tipping-off and compromise potential investigations.

6.1 Assessing Player Behaviour

When assessing the player's risk, IT Management Santora B.V. shall pay special attention to abnormal behaviour such as:

- (a) Large transactions / deposits which are not deemed to be normal for the particular player. This would apply both on the onboarding stage and as an ongoing due diligence monitoring. Since it is a 'large transaction' it is being assumed that the player will automatically qualify for full due diligence obligations since the NAF 4,000 will be reached;
- (b) When a player starts requesting extra secrecy from IT Management Santora B.V. such secrecy request shall be taken into consideration before such player is accepted (Level 1) or is continued to use the company's services when the threshold is met (Level 2). Should such secrecy request is during this level/stage, the Compliance Officer shall be notified immediately and should consider filing an UTR;
- (c) When source of funds and/or source of wealth do not add up to the information provided by the player or if such declarations are difficult to substantiate and/or verify through supporting documentation;
- (d) When the player starts objecting to provide important information at the onboarding stage after reaching the NAF 4,000 threshold, such as identification, verification or any other documents which were requested by the company;
- (e) When the player starts changing his usual betting patterns.
- (f) Furthermore, the player may change the amount he or she usually bets. In such scenarios, the Compliance Officer shall be notified immediately to analyze the situation further and consider any actions that may be taken;
- (g) When the player starts changing the device being used to utilize the company's services or change the IP address / Geo Location. In such situations, it may indicate that the player is using a Proxy or VPN to hide his true location and possibly his true identity. Therefore, in such situations, the Compliance Officer is to be notified immediately irrespective on whether the NAF 4,000 threshold has been reached;
- (h) If an employee feels that a particular player is acting in an abnormal manner which is not listed above, the employee should flag this immediately to the Compliance Officer for further analysis. If there is a suspicion of ML/FT, then the employee shall file an internal Suspicion Transaction Report in line with procedures identified in section 10.1.

In all the above cases, IT Management Santora B.V. shall take extra caution on the player. Any player showing abnormal behaviour will be classified as high-risk if the NAF 4,000 threshold is reached. The Compliance Officer may also decide not to accept the player to continue using the company's service in certain circumstances where the risk profile of the client exceeds the risk tolerance of the business, or due to any other reason known to the Compliance Officer. Such reasons for termination shall be kept on record for at least 5 years following the termination of the player.

6.2 Player Name Screening & Sanctions Screening Procedures

IT Management Santora B.V. shall screen the player for PEP, Sanctions, adverse media and for financial crime at the following situations:

- a. Upon initial registration (before the NAf 4,000 threshold is reached);
- b. Within 30 days after the NAf 4,000 threshold is reached;
- c. At any time if there is a suspicion of ML/FT;
- d. On an ongoing basis in line with the risk-based policy as noted in section 9 subject that the NAf 4,000 threshold has been reached;
- e. On a regular basis in relation to 'Sanctions Screening/Monitoring' to ensure that all players are not sanctioned.

6.2.1 Screening Process and Scope

IT Management Santora B.V. utilises the Sumsub platform to perform automated name screening, forming an integral part of its AML/CFT compliance system. Screening is conducted during onboarding, upon any material change to a customer's profile, and throughout the lifecycle of the business relationship.

The process begins with the collection of customer identification information:

- For individuals: full legal name, date of birth, nationality, and identification document details;
- For legal entities: company's legal name, registration number, and the identities of its directors and ultimate beneficial owners (UBOs).

Sumsub automatically screens this information against a comprehensive range of global databases, including:

- International sanctions lists (UN, EU, OFAC, UK HMT, and the Kingdom of the Netherlands);
- Global PEP databases and enforcement watchlists;
- Adverse media sources, scanning international and local outlets for links to financial crime, corruption, terrorism, or other reputational risks; and
- Custom or internal watchlists, where applicable.

Fuzzy matching algorithms are employed to detect transliterations, aliases, and partial name matches, enhancing detection accuracy.

6.2.2 Review and Escalation

Screening results are automatically classified by Sumsub:

- No match: the player is cleared to proceed through standard onboarding.
- Potential match: flagged for manual review by the Compliance Team.

The Compliance Team verifies flagged results using supporting identifiers (e.g., date of birth, nationality, document details, and biometric data) to confirm whether the match is a false positive or a true positive.

Where a true positive is identified (e.g., sanctions-listed person or high-risk PEP), an internal risk assessment is conducted to determine the appropriate response. Depending on the findings, IT Management Santora B.V. may restrict or terminate the relationship, freeze funds, or escalate the matter. All confirmed high-risk cases are escalated to the Compliance Officer [Gabriela Xuereb] and/or her Team, who evaluates whether an Unusual Transaction Report (UTR) should be filed with the relevant authorities. In cases involving PEPs or individuals linked to adverse media, Enhanced Due Diligence procedures are applied. These procedures include obtaining proof of source of wealth, enhanced identity verification (e.g., second ID document or biometric verification), and increased transaction scrutiny. All flagged cases are documented in the compliance monitoring system and retained in line with legal obligations.

6.2.3 Sanctions & Proliferation Financing Controls

IT Management Santora B.V. complies with the Sanctions National Ordinance (Sanctielandsverordening) and any subsequent implementing decrees, including the *Landsbesluit aanwijzing toezichthouders Sanctielandsverordening* (No. 2024/047237, 28 April 2025), and the Kingdom Sanctions Act (Rijkssanctiewet). The Company ensures that no player, transaction, or business relationship involves sanctioned individuals, entities, or jurisdictions subject to asset freezes or restrictive measures issued by the UN, EU, OFAC, or the Kingdom of the Netherlands.

All clients are re-screened daily against updated sanctions lists to identify new exposures to Targeted Financial Sanctions (TFS) related to terrorism or Proliferation Financing (PF). In cases of confirmed matches, immediate escalation occurs to the Compliance Officer for potential asset freezing, relationship termination, and regulatory reporting.

IT Management Santora B.V. also applies controls to detect and prevent PF risks, which may arise from the use of funds, technology, or materials related to weapons of mass destruction. Heightened scrutiny is applied to jurisdictions and industries associated with weapons manufacturing, dual-use goods, or those designated by the UN Security Council. Any suspicious transaction, pattern, or activity linked to PF must be reported immediately to the Compliance Team.

6.2.4 Ongoing Monitoring and Record-Keeping

Sumsub provides daily re-screening of all active clients. Alerts are generated in real time if a client becomes sanctioned, is newly identified as a PEP, or appears in adverse media. The Compliance Team reviews each alert, documents the outcome, and escalates material cases as required. Inactive clients are re-screened upon reactivation or next transactional activity.

All screening activities including system alerts, manual reviews, and decision rationales—are securely stored within Sumsub for a minimum of five (5) years, ensuring a full audit trail in compliance with Curaçao law. The system adheres to GDPR and ISO 27001 standards and undergoes an annual review to ensure continued effectiveness and regulatory alignment.

6.3 The Risk Assessment

The risk model of IT Management Santora B.V. provides a detailed risk assessment. The below information provides a detailed explanation of the logic behind the risk model (Customer Risk Assessment). Further detail may be found within the 'Business Risk Assessment' of the Company.

The final risk score of a player shall be based on the following after taking into consideration the average risk across all risk types.

Total Score	Risk Level
0 – 50	LOW RISK
51 – 69	MEDIUM RISK
70 +	HIGH RISK

6.3.1 Customer Risk Scoring

IT Management Santora B.V. applies the following combinations when providing scoring for customer risk. This takes into consideration the PEP status, adverse media, sanctions as well as the nationality of having a local resident or otherwise a non-resident. It also takes into consideration the override function for certain types of risks such as sanctions and PEPs as noted below:

Customer Type	Score
Client is PEP	50
Client not PEP	10
Client Sanctioned	50
Client not Sanctioned	10
Client has Adverse Media	50
Client has no Adverse Media	10
Authenticity issues noted	50
No Authenticity Issues noted	10
Single source of income	10
Multiple sources of income	13
Reluctant to provide Due diligence	50
Wealth from high-risk sources ¹	50
Wealth not from high-risk Sources	10

6.3.2 Channel Risk Scoring

The company uses the following scores for interface/delivery channel risk:

Type	Score
Non-Face-to-Face	20

¹ Please refer to section 6.3.7

Non-Face-to-Face using digital ID&V and Biometric Verification (Sumsu)	10
--	----

No override settings exist in this type of risk assessment

6.3.3 Funding Risk Scoring

IT Management Santora B.V. identified the following payment methods. The scoring for such methods is applied as follows:

Funding Type	Score
Skrill	13
Neteller	13
Muchbetter	13
Instadebit	10

6.3.4 Product or Service Risk Scoring

IT Management Santora B.V. shall use the following scoring for the respective services provided:

Product Type	Score
<u>Casino Games</u>	
Slots	10
Roulette	13
<u>Live Casino Games</u>	
Blackjack	20
Roulette	13
Baccarat	20
Poker Cash Game	20
Poker Tournament	13
<u>Sportsbook</u>	
Football	13
Basketball	13
Tennis	13
American Football	13
Ice Hockey	13
<u>Virtual Sports</u>	
Virtual Football	13

Virtual Cycling	13
Virtual Horse Riding	13
Virtual Greyhounds	13
Virtual Drag Racing	13
Virtual Tennis	13
e-Sports	
Counter Strike	13
Call of Duty	13
StarCraft	13
Halo	13
e-Football	13
e-Basketball	13

6.3.5 Geographical Risk Scoring

Countries are scored as follows:

Country Classification	Score
Birthplace is Low Risk Country	10
Birthplace is Medium Risk Country	13
Birthplace is High Risk Country	20
Birthplace is Non-Reputable Country	50
Residency in Low-Risk Country	10
Residency in Medium Risk Country	13
Residency in High-Risk Country	20
Residency in Non-Reputable Country	50
Vested Interest in Low-Risk Country	10
Vested Interest in Medium Risk Country	13
Vested interest in High-Risk Country	20
Vested interest in Non-Reputable Country	50

Since the company identifies several different country risk profiling methods within a client, the highest geographical risk score will be used for the calculation of the final risk score, namely:

- Country of Residency of the player;
- Nationality of the player;
- Countries in which the player declared a vested interest.

One should also note that the following countries have an 'override' condition attached to them, and therefore, when these countries are involved, the player will always be considered as 'High Risk' and this would ensure EDD is performed, subject that the NAF 4,000 is reached. The following jurisdictions are listed as jurisdictions having deficiencies within their AML regime with FATF and/or the European Commission. Furthermore, as noted below.

Iran, Myanmar and North Korea are considered as non-reputable jurisdictions with an international 'Call for Action' status. The company shall not onboard players being exposed to Iran, Myanmar or North Korea.

FATF:²

- Algeria
- Angola
- Bolivia
- Bulgaria
- Cameroon
- Côte d'Ivoire
- Democratic Republic of Congo
- Haiti
- Kenya
- Lao People's Democratic Republic
- Lebanon
- Monaco
- Namibia
- Nepal
- South Sudan
- Syria
- Venezuela
- Vietnam
- Virgin Islands (UK)
- Yemen

European Commission:³

- Afghanistan
- Algeria
- Angola
- Bolivia (effective date from 29th January, 2026)
- British Virgin Islands (effective date from 29th January, 2026)
- Cameroon
- Cote D'Ivoire
- Democratic Republic of the Congo
- Haiti
- Iran
- Kenya
- Laos
- Lebanon
- Mali
- Monaco
- Myanmar

² <https://www.fatf-qafi.org/en/countries/black-and-grey-lists.html>

³ https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-counteracting-financing-terrorism-international-level_en

- Namibia
- Nepal
- North Korea
- Russian Federation (effective date from 29th January, 2026)
- South Sudan
- Syria
- Trinidad and Tobago
- Vanuatu
- Venezuela
- Vietnam
- Yemen

The Compliance Officer shall ensure the above list is kept up-to-date and any active player's jurisdiction risk is updated accordingly, subject that such player reached the NAf 4,000 in relation to information that will be obtained at such level. Any update in the above lists is to be communicated to the risk management and compliance teams. The respective teams shall update the Compliance Officer should there are existing and active players who are exposed to countries added to such lists.

6.3.6 Other Risk Scoring

IT Management Santora B.V. shall ensure the following risk exposures are captured within the customer risk assessment:

Risk Factor	Score
Attempt to use fake documentation	50
Attempt to open multiple accounts from same location	50
Abnormal betting pattern identified	50
Deposit/withdrawal requests without explanation	50
Attempted payment by third party	50

6.3.7 High Risk Source of Funds

Upon reaching the NAf. 4,000 a player is asked to verify his or her source of income. As noted in section 6.3.3 above, the customer risk pillar takes note on whether the player's income is derived from high-risk sources. The below is the list of sources which is considered as 'high risk' by the company:

- Adult entertainment industry
- Oil & Gas industry
- Manufacturing or Printing of Currencies
- Providing a service to the Military
- Manufacturing of Weapons
- Sale or promotion of weapons

- Cryptocurrency or Blockchain
- Cash intensive businesses

Should a player's income be derived from any of the above, this will override the player's risk classification to 'High Risk'. In such a scenario, EDD shall be performed within 30 days from when the Naf. 4,000 are met or from when the company notes such exposure and updated with risk classification.

6.4 Residency of Players allowed to use IT Management Santora B.V.'s services

IT Management Santora B.V. adopts a risk-based approach in servicing clients across different jurisdictions. The target market is defined as follows:

- **Low-Risk jurisdictions:** Accepted with a medium servicing risk
- **Medium-Risk jurisdictions:** Accepted with a medium servicing risk
- **High-Risk jurisdictions:** Accepted with a high servicing risk
- **Non-Reputable jurisdictions:** Generally avoided, with a very low servicing risk

Additionally, IT Management Santora B.V. under no circumstances should service players coming from the following jurisdictions, irrespective of the colour-coded zones:

Web	Mobile
Afghanistan	AF
Argentina	AR
Aruba	
Antigua and Barbuda	AG
Australia	AU
Austria	AT
Belgium	BE
Belarus	BLR
Bonaire	
Brazil	BR
Bulgaria	BG
Cayman Islands	KY
China	CN
Colombia	
Curacao	CW
Croatia	HR
Cuba	CU
Cyprus	CY
Czech Republic	CZ
Denmark	DK
Estonia	EE
France	FR
French Guyana	GY
French Polynesia	PF
French Southern Territories	TF
Guadeloupe	GP
Georgia	GE
Germany	DE
Greece	GR
Hong Kong SAR	HK
Hungary	HU
Iran	IR

Iraq	IQ
Ireland	IE
Isle of Man	IOM
Israel	IL
Italy	IT
Japan	JP
Kahnawake	
Latvia	LV
Libya	LY
Lithuania	LT
Macau	MO
Malta	MT
Martinique	MQ
Mayotte	YT
Mexico	MEX
Monaco	MC
Myanmar	MM
Nigeria	NGA
Netherlands	NL
Netherlands Antilles	AN
North Korea	KP
Norway	NOR
Ontario	CA-ON
Peru	
Philippines	PH
Poland	PL
Portugal	PT
Romania	RO
Réunion	RE
Russia	RU
Saba	
Saudi Arabia	SA
Serbia	RS

Singapore	SG
Slovenia	SVN
Slovakia	SK
South Africa	ZA
Spain	ES
St. Eustatius	
ST. Maarten	
Sudan	SD
South Sudan	SS
Sweden	SE
Switzerland	CH
Syria	SY
Turkey	TR
Uganda	UG
United Kingdom	GB, UK
United States	US
Vatican City	VA
Yemen	YE

IT Management Santora B.V. restricts customer access in certain jurisdictions due to regulatory, ML/TF risks, sanctions, and business risks. Geolocation IP detection blocks registration and gameplay, and deposits or player-to-player transfers are prohibited. Existing customers visiting restricted jurisdictions may withdraw funds, subject to Customer Due Diligence, and access Responsible Gaming tools, where permitted. Employee test accounts are exempt, but deposits, withdrawals, and transfers remain prohibited while in restricted jurisdictions.

7.0 Client Due Diligence and Identification Procedures

IT Management Santora B.V. operates both as a Business-to-Consumer (B2C) and Business-to-Business (B2B) service provider. However, from a B2C perspective, the company exclusively engages with natural persons (individual players).

7.1 Due Diligence Procedures on Natural Persons (Players)

IT Management Santora B.V. shall obtain the following information to ascertain the true identity of the natural persons:

- (a) Official full name;

- (b) Date of birth;
- (c) Permanent residential address;

Before the Naf. 4,000 is reached, and:

- (d) Identity reference number were available;
- (e) Place of birth; and
- (f) Nationality

within 30 days after the Naf. 4,000 is reached. Such process was further described in section 6.

Following the reaching of the Naf. 4,000, the identity of the player shall be verified. The company may decide to verify the identity through technological means before the Naf. 4,000 at its discretion.

In order to verify the client's identity, IT Management Santora B.V. shall request the client to present a copy of a valid identification document which is issued by an independent and reliable source that carries the client's photo (e.g. Passport, National Identity card, Driving Licence, Residency Card etc.). The company may ask for more than one type of identification document as a mitigation measure or if in doubt about the authentication of a document.

After the company is satisfied of the player's identity from the document presented, it will keep scanned copies on the player's file in line with the company's retention policy as noted in section 11. The company is expected to utilise technological tools through a centralised platform known as Sumsub in order to verify the authenticity of a document.

The player's permanent address shall be verified by the production of a recent (up to 6 months) bank statement, utility bill, letter from a public authority, rental agreement, or any other document which verifies the residential address of the player. There is no need to seek an additional verification of address if the address of the player is on his or her identity document and such address matches that declared in the player registration form. The company may opt to use alternative ways to verify the player's residential address as long as such methods would be allowed by Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, and other local rules and regulations.

The above-mentioned information is also essential for implementing the financial sanctions imposed against various persons by the United Nations, European Union and OFAC. In this respect, the passport number, issuing date and country; as well as the client's date of birth should always appear on the documents obtained, so that the company would be in the position to verify precisely whether a player is included in the relevant list of persons subject to financial sanctions. For a more detailed procedures on name screening and sanctions screening please refer to section 6.2.

It is the company's policy to ask the player to verify that he or she is not acting on behalf of a third party. If acting on behalf of a third party, the company shall automatically reject the player. Such declaration shall be part of the player's registration.

7.2 Non face to face meetings

When dealing with non-face-to-face players, the company shall ask for a **scanned copy** of the required documentation. IT Management Santora B.V. shall not require the original documents when only a scanned copy is received. Furthermore, the company may opt to apply technological measures as part of the procedure, as noted in section 6.2.

7.3 Politically Exposed Persons – PEP's

The Company shall ask the player whether he, she, or their immediate family members and close associates are classified as a PEP. The below mentioned definition (or similar) is to be made available to the individual who is responding the question.

The definition of Politically Exposed Persons (PEPs) as provided in a report by the Centrale Bank Curaçao & Sint Maarten closely aligns with the definition set out in the FATF Recommendation 12. It defines PEPs as foreign or domestic persons who are or have been entrusted with prominent public functions and the direct family members or close associates of such persons. PEPs are also persons who are or have been entrusted with a prominent function by an international organization as members of senior management, i.e., directors, deputy directors and members of the board or equivalent functions and the direct family members or close associates of such persons. It is to be noted that the definition of PEP is not intended to cover middle or more junior ranking positions. For the purposes of our customer acceptance process, the company is required to apply EDD in relation to PEPs whether residing in Curacao or abroad.

Examples of PEPs are Heads of State or of government; senior politicians; senior government such as ministers and deputy or assistant ministers; judicial officials such as members of (supreme) courts, of constitutional courts or of other high-level judicial bodies; military officials such as high ranking officers in the armed forces; members of the Council of Advice (Raad van Advies) and the General Audit office (Algemene Rekenkamer); senior executives of state owned corporations and important political party officials.

Examples of direct family members of PEPs are the spouse; any partner as equivalent to the spouse; the children and their spouses or partners; the parents. Examples of close associates of PEPs are natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP; natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the PEP.

IT Management Santora B.V. adopts the following additional measures in relation to PEPs:

Upon registration, the company shall screen the player for a PEP. It is being noted, that whilst the company opted to screen at the initial level of registration, Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction defines such obligation to be initiated within 30 days from when the Naf. 4,000 or equivalent in case of deposit is reached. At each level (Level 1 and Level 2 as described in section 6, the following procedure shall be followed by all staff:

- The Compliance Officer shall be notified and approves to deal with such a PEP before the player is allowed to continue utilising the company's services; (for both level 1 and level 2) and
- Take adequate measures to establish the source of wealth and the source of funds together with supporting documentation; (only at level 2) and
- Conduct enhanced ongoing monitoring (only at level 2).

7.4 Reliance on other subject persons or third parties

Whilst it is highly unlikely that the company places reliance on third parties, these procedures are being provided as guidance for the company and/or its employees should reliance be applied in the future.

The company may rely on CDD measures undertaken by other subject persons or third parties in relation to:

- Identification and verification of an applicant for business;
- Identification and verification of beneficial owner and controlling parties; and
- Information on the purpose and intended nature of the business relationship.

However, the company cannot rely on the ongoing monitoring measures carried out by another subject person or third party. Reliance on CDD procedures undertaken by other service providers is subject to following conditions on the service provider:

- Service provider's consent;
- Agreement to provide information or data immediately after requested and not later than 5 working days; and
- Agreement to retain relevant information and data for at least five years from the request.

The above can be obtained through a Reliance Letter signed by the third party that the company is relying on IT Management Santora B.V. shall sign at least one reliance letter with the third-party making reference to a player list that such a letter covers. The reliance letter or agreement shall be signed by both parties.

Therefore, notwithstanding the fact that IT Management Santora B.V. can place reliance on another entity, the company must obtain the details of the identity of the applicant for business (the player) and information on the purposes and intended nature of the business relationship.

Who qualifies as a third party?

In the context of the licence granted by the Curaçao Gaming Authority (CGA) under the Landsverordening op de Kansspelen (LOK), the License Holder must ensure the following with respect to third-party arrangements:

- Outsourcing:* Where any activity is outsourced to a third-party provider (including, but not limited to, the development, operation, or maintenance of the gaming platform; the provision of games or gaming content; or payment processing and financial

transaction services), the License Holder shall take all appropriate measures to ensure that the third party complies with all applicable laws, regulations, and CGA licence conditions (CGA Licence Conditions, Article 3(2)).

- b) *Game Certification*: Any remote game of chance offered by the License Holder which is supplied by a third-party provider must be certified for soundness and integrity by a testing laboratory approved by the CGA (CGA Licence Conditions, Article 10(2)).
- c) *Disclosure Obligation*: The License Holder must disclose on the CGA's online portal the identity of all third-party game suppliers engaged. (CGA Licence Conditions, Article 10(3)).

Casinos may rely on third parties to perform specific elements of Customer Due Diligence (CDD), provided that certain conditions are met. This reliance does not transfer the responsibility for compliance; the License Holder remains ultimately responsible for adhering to all AML/CFT obligations. Under the Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction, reliance on third parties is permitted when the following criteria are satisfied:

- The casino must obtain, immediately and without delay, the information concerning elements (a)–(c) of the CDD measures outlined in paragraph II.2 of the Regulations.
- The casino must have a formal written agreement with the third party confirming that copies of identification data and other relevant CDD documentation will be made available upon request. This arrangement should be periodically tested to ensure functionality. The casino, however, remains responsible for performing its own customer risk assessment, determining PEP status, and conducting ongoing monitoring.
- The casino must ensure that the third party is regulated, supervised, or monitored for AML/CFT compliance and maintains effective CDD and record-keeping systems. The third party must have an existing, independent business relationship with the customer and apply its own procedures for CDD.
- When determining in which countries the third party may be based, the casino should consider country risk, including the jurisdiction's AML/CFT effectiveness and level of supervision.

A jurisdiction is considered reputable when it has appropriate legislative measures in place for the prevention of money laundering and terrorist financing. In assessing this, IT Management Santora B.V. should refer to:

- Membership or accreditation in recognised international bodies such as the Financial Action Task Force (FATF); and
- Mutual evaluation reports or public statements issued by the FATF or related regional bodies concerning that jurisdiction.

8.0 Information on the purposes and intended nature of the business relationship

Once the applicant for business (the player) has been identified and verified, IT Management Santora B.V. shall also obtain information on the intended nature of the business relationship in order to be able establish the business and risk profile of the applicant for business. Due to the nature of its business, one can easily note that the intended nature of the business relationship shall always be to utilise the betting services provided by the company.

Such procedure shall be triggered upon the player reaching the Naf. 4,000 as described in more detail in section 9.1. Upon reaching such threshold, the company shall obtain the following information from the player within a 30-day period from when such threshold was reached.

8.1 Personal Details of the player

When a customer wishes to create an account, they will be required to complete fields requesting personal information from them for online gambling. Information required from the customer includes:

PERSONAL DETAILS

- Full Name and Surname
- Your Identity Number
- Date of Birth (key in ensuring the player is over the legal age of play in their jurisdiction of residence)
- Place of Birth
- Nationality
- Do you have multiple Citizenships? If so, please provide details.
- Permanent Residential Address
- Current Country of Residence
- Please list any country in which you have a vested interest. Note: this includes any country which you have ties with, or your wealth is generated within such countries, or your own businesses in such countries.
- Your Mobile Phone Number
- Your Email Address

Customers must validate their email address during registration. A unique player ID is assigned to prevent multiple accounts under similar names.

IT Management Santora performs automated checks at registration, including:

- IP address location
- Jurisdiction of residence
- Email uniqueness (one account per user)
- Password duplication (hashed comparison triggers review by Customer Care)

System-generated flags, audit trails, and timestamped logs are maintained for all registration steps, including verification processes and document submission. All customer data is handled in accordance with the Data Protection Policy and Terms of Service. Customers may begin gameplay only after successful registration and verification against relevant databases.

8.2 Source of Wealth and Source of Funds

Establishing the source of wealth and source of funds is particularly important in connection with high-risk players, although reasonable measures should be taken to identify the source of wealth of all players once they reach the NAf. 4,000 or equivalent in case of deposits. The Company shall obtain the following information from the player following the deposit threshold trigger:

Please provide the source of the deposits you have placed with us by indicating below:

- ➔ Savings
- ➔ Inheritance
- ➔ Gift
- ➔ Sale of assets
- ➔ Dividends
- ➔ Other source: Please specify

Please select your current employment status:

- ➔ Full Time Employed
- ➔ Part Time Employed
- ➔ Full Time Student
- ➔ Self-Employed
- ➔ Unemployed
- ➔ Retired

Unless you are unemployed or retired, please provide your current occupation:

Unless you are unemployed or retired, please provide your employer's name and address:

Kindly indicate your annual total income in NAf equivalent:

- ➔ Less than 20,000 NAf
- ➔ 20,001 to 40,000 NAf
- ➔ 40,001 to 100,000 NAf
- ➔ 100,001 to 200,000 NAf
- ➔ Over 200,000 NAf

Please confirm whether you have a single or multiple sources of income:

- ➔ Single Source
- ➔ Multiple Sources

Your Source of Wealth

Please provide an estimate of your net worth (NAF equivalent).

- ➔ 0 to 100,000 Naf
- ➔ 100,001 to 500,000 Naf
- ➔ 500,001 to 1,000,000 Naf
- ➔ Over 1,000,000 Naf

Please indicate what assets form your wealth:

- ➔ Cash at bank
- ➔ Investment products

- ➔ Virtual Assets
- ➔ Real Estate
- ➔ Inheritance
- ➔ Other – please specify

Please select the below if your wealth has been generated through:

- ➔ Cash intensive activities
- ➔ Arms trade, defence or mining activities
- ➔ Cryptocurrencies / Virtual Assets
- ➔ None of the Above

Please explain in detail how your wealth was accumulated:

Where a transaction is perceived to be inconsistent with the source of wealth of the player, additional documents must be requested from the client to justify the transaction. Such additional documentation may include, for example, contracts, agreements for lease or sale, wills, asset and income declarations and other documentation as may be relevant.

8.3 Expected Future Deposits

Following the reaching of the deposit threshold, the player shall be asked to provide an indication of future deposits (monthly average) that he or she expects to deposit with the company.

The company shall ask players who reached the said threshold to provide such information as follows:

Please provide an indication on the expected amount you will deposit with us on a monthly basis in Naf equivalent:

- ➔ 0 to 500 Naf
- ➔ 501 to 1000 Naf
- ➔ 1001 to 3999 Naf
- ➔ 4000 to 6000 Naf
- ➔ Over 6000 Naf

8.4 Player Declarations

Upon reaching the Naf. 4,000, the player shall be asked to provide the following declarations within 30 days from when the said threshold is reached:

1. Please confirm whether you or your immediate family are Politically Exposed Person(s) (PEP):

Definition of a PEP:

The term 'politically exposed persons' is broad and generally includes all persons who fulfil a prominent public function. The Regulations for the combating of Money Laundering, the Financial of Terrorism and Proliferation of Weapons of Mass Destruction distinguishes Foreign, Domestic and International Organisation PEPs as follows:

Foreign PEPs: Individuals holding prominent roles in a foreign country, such as Heads of State, senior politicians, senior government, judicial, or military officials, senior executives of state-owned corporations, and key political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

Persons who are or have been entrusted with a prominent function by an **international organization** refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions

The above list is not exhaustive. Immediate family members of a PEP such as spouse, children, spouses of children and the parents are also considered as PEPs. Close associates of PEPs, such as being shareholders or in business with a PEP are also considered as PEPs.

- ➔ I confirm I/we am/are not a PEP
- ➔ I confirm I/we am/are a PEP

2. I hereby confirm the personal details provided are true and correct

- ➔ I confirm
- ➔ I do not confirm (please provide details)

3. I hereby confirm I have never been convicted of any offence other than minor contraventions related to the use of motor vehicles

- ➔ I confirm
- ➔ I do not confirm (please provide details)

4. I have never been the subject of an investigation by a governmental, professional or other regulatory or statutory body

- ➔ I confirm
- ➔ I do not confirm (please provide details)

5. I have never been incapacitated and have full authority and rights to enter into any contract without restriction

- ➔ I confirm
- ➔ I do not confirm (please provide details)

6. I confirm that I am not representing, acting or placing bets on behalf of a third party.

- I confirm
- I do not confirm (please provide details)

Any match or possible match to a PEP (using the third-party databases) requires to be approved by the Board of Directors. Should approval be granted for a PEP relationship, EDD may be required (such as additional documentation) but all PEPs will also be subject to ongoing monitoring of their account activity. This will be undertaken on a weekly basis to ensure the customer's account is operating as expected and there are no changes to account activity and / or behaviour.

9.0 Ongoing Monitoring Process

Due to the nature of the business, IT Management Santora B.V. is expected to have business relationships which would trigger the ongoing monitoring obligations.

The below ongoing monitoring obligations are triggers upon reaching the NAf. 4,000 or equivalent in case of deposits:

High Risk: At least once Yearly
Medium Risk: Once every 2 years
Low risk: Once every 3 years

Ongoing due diligence may be conducted more frequently than the timeframes mentioned above if it merits on a case-by-case basis or/and if it is requested by the Compliance Officer. Furthermore, such ongoing monitoring on a player would cease should the player be terminated or if the player's account is turned into an 'inactive' status.

It is the company's policy to perform an enhanced review of the player when suspicious transactions or activity are detected. The review shall be performed with immediate effect following flagging of suspicious activity, irrespective of the planned review date of such player.

Following the initial risk assessment of the player after reaching the threshold, ongoing monitoring will enable to identify unusual transactions which may involve money laundering or funding of terrorism. It is noted that certain transaction monitoring is performed since registration and are not linked to the said threshold.

Ongoing monitoring includes:

- (a) Scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the company's knowledge of the player and his or her risk profile including, where necessary, the source of funds and source of wealth. Information on the source of wealth and source of funds should be determined initially (within 30 days of reaching the NAf. 4,000 or equivalent in case of deposits) and on an ongoing basis after applying a risk-based approach; and
- (b) Verifying that the documents, data or information which the company holds are kept up to date and not expired; and

- (c) IT Management Santora B.V. must ensure that the risk status of the player did not change;
and
- (d) Other ongoing monitoring procedures as noted in section 5.3.

Special attention will be taken on any large, unusual complex transactions or unusual patterns of transactions. Activities which are not in line with the risk profile of the player must be brought to attention of the Compliance Officer immediately to ensure that proper action is taken.

9.0.1 Updating missing due diligence of Players

As part of the ongoing monitoring procedures, the compliance team shall check that all players have their respective due diligence file in order. In cases where the file is found to contain missing information and/or due diligence documentation, the following procedure shall take place.

- ➔ The Compliance Officer is informed in writing;
- ➔ The compliance team shall seek the additional information and give the player 30 days to provide the missing information;
- ➔ The Compliance Officer shall decide whether the missing information shall result in temporary suspension of the customer until due diligence is fully in place or otherwise to allow the continuation of the service for a limited time until due diligence is provided;
- ➔ Once the missing due diligence is received, it shall be scanned and uploaded to the customer's file;
- ➔ If due diligence is not received within 30 days, the player shall be suspended or terminated and any funds on account shall be returned to the player by the same channels they were originally received.

9.1 Timing of CDD procedures

CDD measures are applied by IT Management Santora B.V. in the following cases:

Upon registration, the player shall provide minimum identification details but there will be no need to verify such details unless the Naf 4,000 is reached as noted in section 9.1.1 below.

For the sake of clarity, the following situations are being noted when CDD procedures would apply:

- a) New players upon reaching the Naf 4,000 as noted in 9.1.1 – CDD shall be applied within 30 days from such threshold is reached;
- b) Players when carrying out an occasional transaction which is of a value of Naf. 4,000 or more;
- c) Existing players who already reached the Naf 4,000, at appropriate times and on a risk-sensitive basis, including at times when IT Management Santora B.V. becomes aware that the relevant circumstances surrounding a business relationship have changed; and
- d) Existing players whenever doubts arise about the veracity or adequacy of the previously obtained customer identification information, data or documentation.

9.1.1 Analysing the Naf 4,000 and Naf 5,000 Thresholds

The company should have in place systems to monitor the deposits from a player under ALL platforms offered by the company under the Curacao License. The system shall calculate all the deposits of the player at the end of each day and ensure that neither the Naf 4,000 threshold nor the Naf 5,000 threshold has been reached or exceeded.

- Naf 4,000 Threshold shall trigger CDD.
- Naf 5,000 per gaming day threshold shall trigger reporting to the FIU.

IT Management Santora B.V. utilizes the *Umbrella Monitoring System* as its primary transaction monitoring solution. *Umbrella* is a comprehensive and automated tool that continuously monitors client transactional activity and aids in detecting and flagging potentially suspicious behaviour. The system is designed to identify irregularities such as unusual transaction patterns, high-risk jurisdictions, structuring, or other red flags associated with money laundering or terrorist financing. When specific predefined thresholds or scenarios are triggered, the system automatically generates alerts.

Once generated, alerts are first reviewed by the Risk Team, who acts as the first line of defence in this process. The team evaluates each alert to determine its relevance, urgency, and risk level. In addition to processing system-generated alerts, the Risk Team also conducts ad-hoc monitoring in response to specific concerns or risk indicators, particularly with respect to high-risk clients or transactions with no clear economic rationale.

Where further investigation is deemed necessary, the Risk Team initiates a Jira task and assigns it to the Compliance Officer for comprehensive analysis. This includes a detailed review of the client's KYC file, historical transactions, supporting documentation, and any other relevant information. Based on this assessment, the Compliance Officer determines whether the alert can be closed, requires continued monitoring, or necessitates the submission of an Unusual Transaction Report (UTR) to the Financial Intelligence Unit (FIU).

All actions and decisions taken throughout the monitoring process are documented within the Jira platform to ensure a robust and auditable compliance trail. This approach ensures accountability and provides evidence of compliance with regulatory requirements. The overall transaction monitoring framework at IT Management Santora B.V., including the performance of the *Umbrella* system is subject to periodic internal review and independent audit, as appropriate.

9.2 Simplified Due Diligence

In certain cases, the company may maintain minimal information about the player even after the Naf 4,000 is reached or exceeded. SDD may be applied:

- (a) In relation to activities or services that are determined by the FIU to represent a low risk of money laundering and funding of terrorism; or
- (b) Where, on the basis of the risk assessment carried out by the company, it was determined that any occasional transactions or a business relationship represents a low risk of money laundering and funding of terrorism, even after the Naf 4,000 was reached.

In such cases, the level of due diligence obtained by the player may be of a lower amount, unless there is a change in the risk classification of the player in the future, or the company feels that the information

obtained is not adequate to mitigate against specific risks identified on the player. The company may opt to apply CDD (not simplified) even if the ML/FT risk is low.

9.3 Customer Due Diligence & The Know Your Customer (KYC) Process

The customer onboarding process at IT Management Santora B.V., operating through various online platforms (collectively referred to as the *Platforms*) begins when a prospective user accesses the website and selects the "Register" or "Sign Up" option. The user is prompted to complete a registration form by providing personal details including full name, date of birth, residential address, email address, username, password, and country of residence. Acceptance of the platforms terms and conditions and privacy policy is mandatory. Upon submission, the user receives an automated email with a confirmation link, which must be clicked to activate the account. Once the email is confirmed, the user gains access to their personal dashboard. At this stage, the platforms initiate Know Your Customer (KYC) procedures as required under Curaçao's AML/CFT framework, via Sumsb. Until verification is completed, the customer's account is subject to provisional restrictions, such as deposit and withdrawal limits or betting caps, to mitigate financial crime risks. This process ensures that all customers are appropriately identified and screened before full access to the platform's services is granted.

Then, users are required to submit all relevant documentation necessary to fulfil the applicable Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements. These documents are carefully reviewed and verified by the assigned Risk Manager (RM) to ensure authenticity, completeness, and consistency with the information provided during registration. Once verified, the documents are securely uploaded and stored within the client's dedicated profile in the AGP system, which serves as the central repository for all client due diligence records and ongoing monitoring data.

9.4 Enhanced Due Diligence

IT Management Santora B.V. shall apply EDD in situations which, by their nature, present a higher risk of ML/FT after the NAF 4,000 is reached. Such measures ensure that higher risks are better monitored and managed to avoid involvement in ML/FT.

IT Management Santora B.V. applies EDD when the risk classification of the player is 'High Risk' after taking into consideration all the risks involved as mentioned in section 6.3. Furthermore, the company has designed its customer risk assessment to take into consideration situations where the player will always be classified as 'high risk' due to:

- d) Residents of higher risk geographic areas;
 - e) Being a sanctioned entity or individual;
 - f) Politically Exposed Persons (PEP's);
 - g) Products or transactions that might favor anonymity;
 - h) New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.
-
- (a) Being a Politically Exposed Person; or
 - (b) Being a sanctioned entity or individual; or
 - (c) Individual residing or is a citizen of a set of countries considered by IT Management Santora

- B.V. to represent a higher risk than 'high risk' countries or jurisdictions (as noted in section 6.3.2); or
- (d) The player has its wealth being derived from high-risk sources as noted in section 6.3.7; or
- (e) Other scenarios noted in section 6.3.6.

In such 'High Risk' cases, the company may apply one, or more, of the following measures as a means of EDD:

- 1) Establish the identity of the applicant for business by using additional documentation and information

In such cases a bank reference and professional reference may be obtained. Where such documents do not provide proof of residential address, an additional utility bill or bank statement containing residential address may also be produced.

- 2) Verify or certify the documentation supplied using supplementary measures.

This involves certification for the purposes of verification of identity by a legal professional; notary; accountancy professional; a person undertaking relevant financial business; or a person carrying out an activity equivalent to relevant activity carried out in another jurisdiction. Please refer to Section 7.2 when it comes to certification policy of the company. In other high-risk circumstances, the Compliance Officer will decide on the most appropriate EDD measures.

- 3) Ensure that the first payment of transaction into the account is carried through an account held by the player in his or her name with a credit institution authorised under the Banking Act or otherwise authorised in another member state of the community or in a reputable jurisdiction.

IT Management Santora B.V. shall always obtain supporting documentation on the source of wealth / source of funds when the player has reached the NAF 4,000 as noted in section 9.1.1 and the risk classification of such player is 'high risk'. The company shall also ensure that the source of wealth description provided by the player is detailed.

The table below provides a visual overview of the documentation required in cases where Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) is applied. It is important to note that each customer is unique, and the specific documentation requested may vary based on the individual circumstances of the case.

EDD conducted	Customer Risk		
	Low	Medium	High
World Check review and source review	✓	✓	✓
Facebook		✓	✓
Twitter		✓	✓
LinkedIn		✓	✓
Instagram		✓	✓
Internet News search		✓	✓
Government Websites			✓
Role in public life			✓

Source of Funds			✓
Source of Wealth			✓
Enhanced background report (case by case)	N/A	N/A	As required

10.0 Recognition and reporting of suspicious transactions/activities

IT Management Santora B.V. in cases where there is an attempt of executing transactions which knows or suspects that are related to money laundering or terrorist financing, reports, through the Compliance Officer its suspicion to the FIU Curacao.

The relevant list is not exhaustive, nor it does include all types of transactions that may be used, nevertheless it can assist the company in recognising the main methods used for money laundering and terrorist financing. The detection by the company of any of the transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds, the nature and economic/business purpose of the underlying transaction, and the circumstances surrounding the particular activity.

The company has an automated system in place, that is *Umbrella* which automatically flags to the Risk Team when a transaction of a player or the player's behaviour merits further analysis or monitoring. The automatic system shall trigger red flags in an automated manner based on several rules.

Once a trigger has been flagged to the respective team, an individual from the said team shall review the trigger. If the trigger results in suspicion of ML/FT, then the procedure as described in section 10.1 shall be strictly followed.

10.1 Internal reporting procedures

Employees of the company shall submit an internal UTR to the Compliance Officer of the company immediately after detecting a suspicious transaction. Please refer to Appendix A for a copy of the internal UTR form. The UTR shall be sent directly to the Compliance Officer via email and shall be considered highly confidential. The employee who submitted the UTR should not disclose such information with persons outside the company. Furthermore, the employee shall share such information internally on a need-to-know basis. Such sharing of information shall be limited and avoided in order to reduce the risk of tipping off the player involved in the UTR. The UTR shall be sent to santora@a2co.com on the same day it was raised.

10.1.1 Examples of situations which may lead to the filing of an UTR

The Compliance Officer is expected to file an UTR when and if she has a suspicion of ML/FT after receiving and reviewing an internal UTR. The below scenarios are to serve as an example of situations which may trigger the requirement to file an UTR with the FIU Curacao. That said, it is entirely up to the Compliance Officer to make such decision.

- Player reluctant to provide due diligence documentation after the NAF. 4,000 or equivalent in case of deposit is met;
- When there is doubt about the authenticity of the documents provided;
- When a player deposits large transactions;
- When a player asks for unnecessary level of secrecy;
- When a player provided false information upon registration or after the NAF. 4,000 or equivalent in case of deposit is reached;
- When a player's IP address changes frequently without explanation;
- When a player's Geo Location changes frequently or does not match the country of residency declared upon registration;
- When the betting behaviour of the player changes drastically without valid reasons;
- When the player is using multiple channels to perform a deposit;
- When there is evidence or doubt of collusion between two or more players when playing Poker.

The above list shall be taken as guidance and should not be considered as exhaustive.

10.2 External reporting procedures

Any disclosures made by IT Management Santora B.V. to the FIU Curacao should be made on the same day that the UTR has been raised internally. If due to the complexity of the UTR, the Compliance Officer cannot manage to file an external UTR on the same day, then the Compliance Officer should file the UTR as soon as possible and without undue delay. The filing of the UTR shall take place on the same day or as soon as reasonably possible:

- (a) In cases where, subsequent to the receipt of an internal report, the Compliance Officer determines, on the basis of the information contained in the report, or on the basis of additional information and/or documentation, that there is knowledge or suspicion of ML/FT;
- (b) Notwithstanding the provisions of paragraph (a), where the subject person is in possession of information that constitutes a reasonable ground to suspect ML/FT, the obligation to file the UTR would be initiated since the subject person received such information.

All measures should be taken not to tip-off customers regarding:

- a. the submission of UTRs to the FIU Curacao,
- b. any information demanded by or transmitted to the FIU Curacao within the context of ML/TF analysis and
- c. any ML/TF investigations on a customer

It should be noted that an UTR should only be filed with the FIU Curacao using the GoAML platform and should not be copied to any supervisory authority. After the submission of an UTR, the company may subsequently wish to terminate its relationship with the player concerned for risk avoidance reasons. In such an event, the company shall exercise particular caution, not to alert the client concerned that an UTR has been submitted to the FIU Curacao. Close liaison with the FIU Curacao is, therefore, maintained in an effort to avoid any frustration to the investigations conducted. Furthermore, it is being highlighted that the employee(s) filing an internal UTR shall not be mentioned in the UTR

sent to FIU Curacao by the Compliance Officer. This is to ensure full protection on the individual filing the internal UTR.

If once a report is filed the subject person decides to maintain the business relationship or continues with the execution of the occasional transaction, the company should classify the player as high-risk and monitor the activities of that player to a larger extent.

IT Management Santora B.V. is committed to follow guidance/instructions from the FIU Curacao on a case-by-case basis.

10.3 Obligation to refrain from carrying out a transaction that appears to be suspicious

IT Management Santora B.V. shall not carry out a transaction that is suspected or known to be related to ML/FT until the Compliance Officer has informed the FIU Curacao in line with the above reporting procedures. In compliance with the National Ordinance on the Reporting of Unusual Transactions (LMOT), IT Management Santora B.V. are legally required to report both completed and intended unusual transactions to FIU Curaçao without delay and must retain copies of all submitted UTRs and any supporting documentation for a minimum period of five years.

In the unlikely event that the company is not in a position to refrain from carrying out a transaction which is known or suspected to be related to ML/FT in view of the fact that such action is impossible because of the nature of the transaction or such action is likely to frustrate efforts of investigating or pursuing the beneficiaries of the suspected ML/FT operations, the company shall carry out the transaction and the Compliance Officer inform the FIU Curacao immediately.

For the avoidance of any doubt, if there is a suspicion of ML/FT on a player, such player shall not be allowed to withdraw any funds from his or her account until the account is released by the Compliance Officer following FIU Curacao's instructions.

10.4 Dealing with non-cooperative players

A player is deemed "non-cooperative" when he or she failed to provide due diligence and/or supporting documentation (including that on wealth), as requested by the Company and/or the Compliance Officer, within 30 days from reaching the NAf 4,000 or equivalent in case of deposits, as described in section 9.1.1. Furthermore, the player may be classified as non-cooperative if he or she communicates his or her unwillingness to cooperate with IT Management Santora B.V. before the lapse of the 30 days. In such cases, the company shall follow the following procedure:

- Block the account of the player, including the ability to make deposits & withdrawals
- Inform the Compliance Officer
- Ensure that any amounts on account are blocked and are not sent back to the player until the Compliance Officer's written authorization
- Await for the Compliance Officer's written authorisation to release funds back to player
- In the case where the Compliance Officer provides alternative instructions, the employee is to follow the Compliance Officer's instructions
- In the event where the Compliance Officer has released the funds, the Company shall ensure that funds are sent back through the way it was received. If this is not possible due to technical reasons, the Company shall always ensure that the bank account that

the funds will be sent to has been verified to be in the name of the player and within a reputable jurisdiction (as noted in the latest Country Risk Reports of the company).

11.0 Record-keeping procedures

It is the policy of the company to maintain records of identification (where applicable) and any other documents related to the player in electronic form with the Back Office for the entire period that it is providing a service to the player and for 5 years after such service has been completed or relationship terminated. Record-keeping is also important for the competent authorities who are responsible for the analysis, investigation, and analysis of the possibility of ML/FT. Such records may also be requested by FIU Curacao.

When the company ceases to provide the service to the player, all information related to the player needs to be archived. This information should be destroyed after 5 years from such termination of service with the player in line with the retention policy of IT Management Santora B.V. which is part of the privacy notice provided to players as per GDPR obligations.

The following records need to be maintained:

1. All transactions, deposits, withdrawals, bets and registration details of all players, irrespective of whether the NAf 4,000 was reached;
2. Due diligence documents including evidence of identity and business relationship in respect of all players who reached the NAf 4,000;
3. Records of details relating to the business relationship and all transactions carried out in the course of the business relationship;
4. Records of the findings of the examination of the background and purpose of the relationship and transactions carried out;
5. Evidence of ongoing monitoring of players (where applicable);
6. Evidence of the management of and monitoring of compliance with internal controls;
7. The Compliance Officer will need to keep details of training provided to all personnel to ensure that the staff can detect and treat transactions that may lead to money laundering. Such documentation should include:
 - a) The date on which the training was delivered;
 - b) The nature of the training;
 - c) The names of employees receiving the training;
 - d) The results of any assessments undertaken by employees; and
 - e) A copy of any handouts or slides;
8. Record of the internal reports made to the Compliance Officer should be maintained;
9. Electronic copy of any UTRs maintained by the Compliance Officer in a secured location;
10. Suspicious Transaction Reports (UTRs) submitted to the FIU Curacao;
11. Reasons for not forwarding internal reports to the FIU Curacao (if applicable); and
12. Due diligence documentation on new employees.

12.0 Education

12.1 Employees' education and training policy

The general principles below apply:

- (a) The Compliance Officer shall ensure that employees are fully aware of their legal obligations according to the Law by introducing a training program;
- (b) Timing and content of the training provided to the employees of the various departments will be determined according to the needs of business from time to time. The frequency of the training can vary depending on the amendments of legal and/or regulatory requirements, employees' duties as well as any other changes in the financial system of the jurisdictions in which IT Management Santora B.V. operates;
- (c) The annual training program aims at educating the IT Management Santora B.V.'s employees on the latest developments in the prevention of money laundering and terrorist financing, including the practical methods and trends used for this purpose. This program is revisited on an ongoing basis during the year to reflect new developments; and
- (d) Ongoing training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

All employees should be made aware of the IT Management Santora B.V.'s:

- (a) Customer (player) due diligence measures;
- (b) record-keeping procedures;
- (c) internal reporting procedures;
- (d) policies and procedures on internal control;
- (e) policies and procedures on risk assessment and risk management; and
- (f) policies and procedures on compliance management and communication.

All employees should be informed of the identity of the Compliance Officer and of her functions and responsibilities. Employees should also be made aware of the following:

- (a) National Ordinance on Games of Chance (LOK - Landsverordening op de Kansspelen;
- (b) National Ordinance on Identification when Rendering Services (LID / NOIS - Landsverordening Identificatie bij Dienstverlening);
- (c) Landsverordening Melding Ongebruikelijke Transacties (LMOT / NORUT - National Ordinance On The Reporting of Unusual Transactions);
- (d) Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction;
- (e) Kingdom Sanctions Law (SW - Rijkssanctiewet)
- (f) Sanctions National Ordinance (SNO – Sanctielandsverordening)
- (g) FIU Curaçao Guidance Notes and Typologies (as periodically updated)
- (h) National Decree designating Supervisors under the Sanctions Ordinance (Landsbesluit aanwijzing toezichthouders Sanctielandsverordening, No. 2024/047237)

The training program above shall include practical insights into ML/FT risks as appropriate and shall also be tailored to the company's activities as well as the role and function of different employees. The

Compliance Officer and designated employee shall attend external training as relevant to her responsibilities in the context of the business activities undertaken, that is, remote gaming.

The training provided by the company shall be as follows:

- (a) To new employees during the induction training upon commencement of work related to the 'relevant activity' of the business;
- (b) To specific employees where there is a change in the employees' role at some stage after employment; and
- (c) To all employees including senior management (including directors) on an annual basis or earlier where there is a substantial change in legislation.

The company shall keep record on:

- ➔ The date on which training was delivered;
- ➔ The nature of the training;
- ➔ The names of the employees who received training; and
- ➔ A copy of any training materials provided.

12.1.1 Minimum content of AML Training

Annual AML training should include the following:

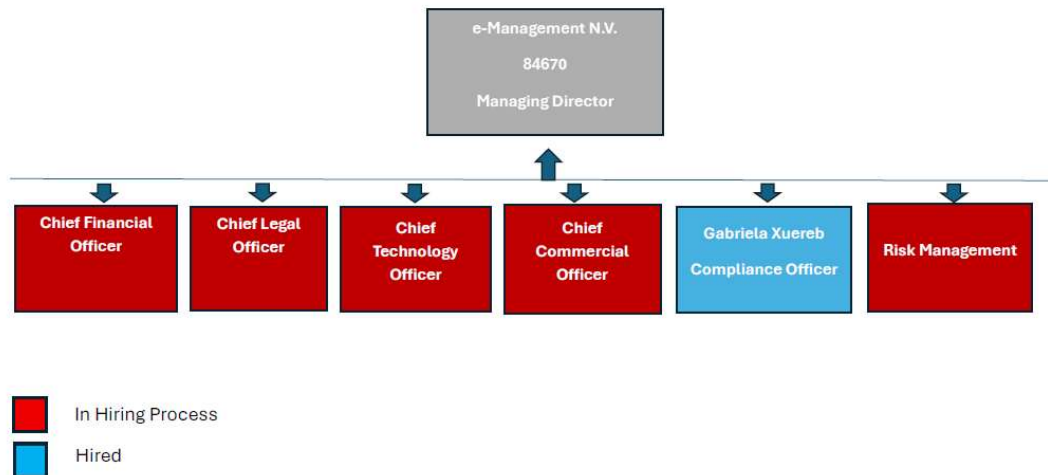
- a) A clear explanation on the timing of CDD for remote gaming companies and the calculation of the NAF 4,000;
- b) Transaction monitoring obligations;
- c) Customer (player) due diligence measures – before and after threshold;
- d) Record-Keeping procedures;
- e) Internal reporting procedures;
- f) The role of the Compliance Officer in filing UTRs with the FIU Curacao (external reporting);
- g) Risk management measures, including:
 - Customer acceptance policies;
 - Customer risk assessment procedures;
 - Internal controls;
 - Compliance management;
 - Communications;
 - Employee screening policies and procedures;
 - Any other relevant policies and procedures concerning AML/CFT
- h) The ML/FT risks posed by the business and/or activities of the subject person (outcomes of the business risk assessment).

12.2 Vetting of new employees

The company shall ensure that new or prospective employees are vetted and fit to perform the relevant activity, that is, Gaming activities. New joiners will be subject to due diligence procedures which would generally include obtaining professional references, confirming employment history and qualifications

and requesting recent police conduct certificate. This requirement is applied irrespective of the position of the employee.

12.3 Ongoing testing of outsourcing providers



The company's sole outsourcing provider is the Compliance Officer, Ms. Gabriela Xuereb, who has been appointed to oversee the compliance function and ensures continuity and oversight in the implementation of the AML/CFT framework.

The company shall ensure the following is in place in relation to outsourcing parties:

- Legal agreements are in place to regulate the relationship between IT Management Santora B.V. and the outsourcing party;
- Ensure that the outsourcing party has the required resources to perform such outsourcing duties;
- Ensure the outsourcing party has the skills, qualifications or training to perform the outsourcing duties;
- Ensure the outsourcing party is in good standing and no adverse information exists and that it is located in a reputable jurisdiction.

As part of its ongoing monitoring of the relationship with the above, the company shall:

- Hold a list of employees of the outsourcing party who directly deal with the outsourcing work;
- Perform name checks or google searches on the third party to ensure no adverse media exists which may have an adverse impact on the company;
- Ensure the outsourcing party is in good standing by obtaining a Good Standing certificate.

The above shall be performed regularly as deemed necessary by the Compliance Officer.

13.0 Approval and updating of AML Manual

This manual shall be approved in writing by the Board of Directors through a Directors' resolution. Such resolution is to be kept on record, together with this version of the manual for at least 5 years following an update of such manual.

This manual may be updated from time to time as required. The following are triggers that may initiate the require for the AML manual to be updated:

- ✓ A change in the AML regulations;
- ✓ A change in an internal policy or procedure in relation to AML or player onboarding;
- ✓ A new requirement by the FIU Curacao;
- ✓ A change in key personnel mentioned in this document, such as but not limited to the FIU Curacao;
- ✓ Any other improvement deemed necessary by the company or the Compliance Officer.

Upon every update, a different version shall be noted. The manual should indicate the updates or changes made from the previous version. The updated manual is to be approved by the Board of Directors in writing by means of a directors' resolution. Such resolution and updated version of the AML manual shall be kept on record for at least 5 years.

14.0 Contact Information

For any questions or clarifications regarding this AML Policy, please contact:

Compliance Officer: Gabriela Xuereb

Email: santora@a2co.com

Telephone: +356 99037357

Office Number: +356 2133 2100

Address: Emancipatie Boulevard Dominico F. "Don" Martina 29 Curaçao

Appendix A – Internal UTR Form

INTERNAL UNUSUAL TRANSACTION REPORT

UTR NO.

****SECRET & CONFIDENTIAL****

As an employee of IT Management Santora B.V., you are using this internal form to report a suspicion or knowledge of Money Laundering or Funding of Terrorism. This report shall be sent directly to the Compliance Officer by email. No other employees shall be copied in the email, and this report shall not be shared.

Report Prepared by:		Date of Report:		
Team/Department:				
Customers Name:				
Username:		Date of Birth:		
Address:				
Postcode:				
Email Address:				
Telephone Number:				
Current balance on A/C:	NAf			
No. of deposits:		Total deposits	NAf	
Deposit method/SOF:				
No. of withdrawals:		Total withdrawals	NAf	
Account status:	Open	Closed	Suspended	Other
Identification and address verification undertaken:				

Enhanced due diligence undertaken:	
------------------------------------	--

Reason for suspicion	
Please provide a full description outlining:	
• Transaction, activity or situation that has aroused your suspicion • Reason for suspicion • Whether criminal conduct is known or suspected • Proposed actions to be taken	

Declaration by person filing this UTR:

I hereby declare that to my best of knowledge, the above information is true, full, and correct. Furthermore, I hereby understand my obligations under the law in relation to tipping off offense. I understand that confidentiality and secrecy in this matter is of utmost importance and that I shall not tip-off the player of this internal report.

Signature and information of Person filing UTR	
Name of Person:	
Designation	
Signature	
Date and Time	

Note:

Beware of tipping off: do not tell the client or anyone else that you have made this report. You will receive a receipt for your report within 48 hours of submission – remember to ask for your receipt if you do not receive it within this timeframe.

For Compliance Officer use only

Receipt of report acknowledged:	
Name of Recipient:	
Designation	

Signature	
Date and time received	

References

- Government of Curaçao. (2017). Landsverordening melding ongebruikelijke transacties (GT). 99. Opgehaald van https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2017_no_99_landsverordening_melding_ongebruikelijke_transacties_gt.pdf
- Caribbean Financial Action Task Force (CFATF). (n.d.). *Documents*. Opgehaald van <https://www.fatf-gafi.org/en/countries/global-network/caribbean-financial-action-task-force--cfatf-.html>
- Curacao Gaming Authority . (2025, April 17). *Responsible Gaming Policy for Licensed Operators* . Opgehaald van <https://portal.cga.cw/uploads/publications/njQTNnLQ58QstzkXO5DB3XC0gE3aDeC29jpLcQLW.pdf>
- FATF. (2012-2025). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Paris, France. Opgehaald van <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf>
- FIU Curacao . (2024). *Regulation on Indicators of Unusual Transactions* . Opgehaald van <https://fiucuracao.org/wp-content/uploads/2025/09/Ministerial-Regulation-2024-no.-60-amending-the-Indicators-unusual-transactions.pdf>
- FIU Curaçao. (n.d.). *Guidance Notes and Typologies*. Opgehaald van <http://www.fiucuracao.cw/web/motweb/motweb.nsf/web/home?opendocument>
- Gaming Control Board. (2025). Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction. Curacao. Opgehaald van https://gamingcontrol.spin-cdn.com/media/aml_cft/20250110_regulations_for_the_combating_of_money_laundering_and_financing_of_terrorism_version_january_10_2025.pdf
- Government of Curacao . (2015). Regeling indicatoren ongebruikelijke transacties, Publicatieblad, no. 73. Opgehaald van https://gamingcontrol.spin-cdn.com/media/pdf_files/20191108_pb_2015_no_73_regeling_indicatoren_ongebruikelijke_transacties.pdf?utm_
- Government of Curacao . (2025). Opgehaald van Landsbesluit aanwijzing toezichthouders Sanctielandsverordening (No. 2024/047237): <https://gobiernu.cw/wp-content/uploads/2025/05/Landsbesluit-aanwijzing-toezichthouders-Sanctielandsverordening.pdf>
- Government of Curaçao. (2013). Landsverordening Bescherming Persoonsgegevens. Opgehaald van https://gobiernu.cw/wp-content/uploads/2019/07/P.B_2013__no._92.pdf
- Government of Curaçao. (2024). Landsverordening identificatie bij dienstverlening. (Publicatieblad (Official Gazette) P.B. 2024, no. 41). Opgehaald van https://gamingcontrol.spin-cdn.com/media/aml_cft/20240517_pb.pdf

Government of Curaçao. (2024). Landsverordening op de kansspelen. 157. Opgehaald van https://gamingcontrol.spin-cdn.com/media/online_gaming/20241230_landsverordening_op_de_kansspelen.pdf

Government of Curaçao. (n.d.). Sanctions National Ordinance (Sanctielandsverordening). Opgehaald van https://gamingcontrol.spin-cdn.com/media/aml_cft/20250110_pb_2014_no_55_gt_sanctielandsverordening.pdf

Government of the Netherlands (Rijksoverheid). (2017). Rijkssanctiewet (Kingdom Sanctions Act). Opgehaald van https://gamingcontrol.spin-cdn.com/media/aml_cft/20250110_wettennl_regeling_rijkssanctiewet_bwbr0038211.pdf

****END OF MANUAL***