AML/CTF AND SANCTIONS COMPLIANCE POLICY

Date of effectiveness: 15.08.2025

Approved on: 15.08.2025 by Director

Prepared by and accepted:	Adrian Olivier Soto Lopez
AML Officer (Name and Surname)	Adrian Olivier Soto Lopez

Any changes in this document must be agreed upon with the AML Officer or the person who fulfils the functions of the AML Officer during his absence.

Contents

DEFINITIONS

AML / Compliance Department - The unit has primary responsibility for the initiation and delivery aspects of the AML program within an Organisation.

Business relationship - Business or commercial relationship between a Customer and the Organisation and which is expected, at the time when the contact is established, to have an element of duration for a certain period (e.g. conclusion of an agreement between the Customer and the Organisation, continuous performance of gambling/betting and monetary operations and transactions).

Close Associate - A natural person who, together with the Politically Exposed Person, is a member of the same legal entity or of a body without legal personality or maintains other business relationship.

Close family member - The spouse, the person with whom partnership has been registered (i.e. the cohabitant), parents, brothers, sisters, children and children's spouses, children's cohabitants.

***Customer due diligence (CDD*)** - Identification of the Customer and verification the Customer's identity on the basis of documents, data or information obtained from a reliable and independent source; assessment and, as appropriate, obtainment of information on the purpose and intended nature of the Business Relationship; the conducting of ongoing monitoring of the Business Relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Organisations' knowledge of the Customer.

Customer/Client/Player - a person that uses online gambling and betting services provided by the Organisation.

FATF – The Financial Action Task Force.

FIU – Financial Investigation Unit.

High-risk third countries - countries identified as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the Union's financial system (Article 9 of Directive (EU) 2015/849).

Identification - A part of Customer Due Diligence, allowing to ascertain the identity of a person on the basis of the personalised unique information directly related to that person.

Law – Law on the Prevention of Money Laundering and Terrorist Financing.

Money laundering (ML) - the doing of any act which constitutes an offence of money laundering and is defined in the Law on the Prevention of Money Laundering and Terrorist Financing of Anjouan. The criminal acts cover all procedures that seek to change the identity of illegally obtained funds, arising from drug dealing, terrorist activities or any other crime in order to give impression that such money originated from legitimate or legal sources. Money laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities such as, for example, fraud, corruption, organized crime, or terrorism etc.

Organisation – Qintara Limitada, the company established under the laws of the Republic of Costa Rica , with its registered address at Provincia 06 Puntarenas, Canton 11 Garabito, Jaco, Costado Este De La Municipalidad Garabito, Bufete Sanchez Chavarria, 61101, Costa Rica. and company number: 3-102-935655, online gambling institution established under the laws of the Republic of Costa Rica and authorized by the Government of the Autonomous Island of Anjouan, Union of Comoros (license number License number) and, therefore, falling within the definition of an institution that falls under the Law on the Prevention of Money Laundering and Terrorist Financing. The term "Company / Organisation'' when used in these Policies also refers to the management bodies of the Organisation and the members of such bodies as well as the employees of the Organisation.

Policy – AML/CFT and Sanctions Compliance Policy.

Politically Exposed Person (PEP) - Natural persons who are or have been entrusted with Prominent Public Functions and Close Family Members or Close Associates of such persons.

Prominent Public Functions*:*

1. The head of the state, the head of the government, a minister, a vice minister or a deputy minister, a secretary of the state, a chancellor of the parliament, government or a ministry;

2. A member of the parliament;

3. A member of the Supreme Court, the Constitutional Court or any other supreme judicial authorities whose decisions are not subject to appeal;

4. A mayor of the municipality, a head of the municipal administration;

5. A member of the management body of the supreme institution of state audit or control, or a chair, deputy chair or a member of the board of the central bank;

6. Ambassadors of foreign states, a charge d'affaires ad interim, the head of Anjouan armed forces, commander of the armed forces and units, chief of defence staff or senior officer of foreign armed forces;

A member of the management or supervisory body of a public undertaking, a public limited company or a private limited company, whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state;

8. A member of the management or supervisory body of a municipal undertaking, a public limited company or a private limited company whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, that are owned by the state, and which are considered as large enterprises

9. A director, a deputy director or a member of the management or supervisory body of an international intergovernmental organisation;

10. A leader, a deputy leader or a member of the management body of a political party.

Source of funds – means the origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship, for

example the customer's salary, as well as the means through which the customer's funds were transferred.

Source of wealth – refers to funds that the customer has acquired during a prolonged period of time and that make up the customer's entire body of wealth (total funds). When determining the source of wealth, the main focus is the acquisition of information on customer's activities that indicate how the customer acquired the wealth.

Terrorist financing (TF) - the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense.

1. SCOPE OF THE POLICY

1.1 As part of the commitment to maintaining the highest standards and following all relevant regulations, it is the Organizations' policy to prohibit and prevent any cases of money laundering and terrorist financing.
Whereas the Organisation is Qintara Limitada, the company established under the laws of the Republic of Costa Rica , with its registered address at Provincia 06 Puntarenas, Canton 11 Garabito, Jaco, Costado Este De La Municipalidad Garabito, Bufete Sanchez Chavarria, 61101, Costa Rica. and company number: 3-102-935655 , online gambling institution established under the laws of the Republic of Costa Rica and authorized by the Government of the Autonomous Island of Anjouan, Union of Comoros (license number License number) and, Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature, or the origin of funds derived from the illegal activities. Money laundering involves not only the proceeds of drugs trafficking, but funds related to other illegal activities, including fraud, corruption, organized crime, terrorism, and many other crimes. Generally, the money laundering consists of three stages:

Placement: introduction of cash originating from illegal / criminal activities into financial or non-financial institutions.
Layering: separating the proceeds of criminal activities form their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.
Integration: placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as legitimate funds.

1.2 Terrorist financing encompasses the means and methods used by terrorist organizations to finance their activities. This money can come from legitimate sources, for example from profits from businesses and charitable organizations. But terrorist groups can also get their financing from illegal activities such as trafficking in weapons, drugs or people, or kidnapping for ransom.

This Policy is developed and periodically updated by the Anti-Money Laundering Officer of Qintara Limitada (the Organization) based on the general principles set up by the Board of Directors of the Organization in relation to the prevention of money laundering and terrorist financing.
The Policy applies to all employees of the Organization and aims to setup key roles and responsibilities for the staff members as well as to ensure compliance with the following legislation:

- European Directive 2005/60/EC and European Directive 2018/843 on the prevention of the use of the Financial System for the purpose of money laundering and terrorist financing as transposed into National Law (L188(I)/2007-2018
- Anjouan Money Laundering (Prevention) Act 008 of 2005.

All amendments and/or changes of the current version of the Policy must be approved by the Company's Board of Directors.

1.3 Responsibilities and Recipients of the Document:

Owner of the process: AML Officer

Responsibilities:

This document is binding to all employees of the Organisation whose job responsibilities are related to establishment and review of the business relationships.

In cases of violations of the Procedure, the detector of the violation immediately informs the head of his structural unit. If differences are found between the processes carried out in the Organisation and those determined in the procedure, the Owner of the process should be informed about this.

Recipients of the Document:

- Customer support department
- Fraud Prevention department
- Payments department
- AML department

2. BOARD OF DIRECTORS

2.1 The Board of Directors is responsible for ensuring that the Organisation complies with its obligations under the Law. The Board shall assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the obligations under the Law, and to take appropriate measures to address any deficiencies.

2.2 The main duties and responsibilities of the Board of Directors in relation to the prevention of money laundering and terrorist financing mainly include:

- Determining, recording and approving the general policy principles of the Organisation in relation to the prevention of money laundering and terrorist financing and inform the Anti-Money Laundering Officer accordingly

- Appointment of an Anti-Money Laundering Officer and determining his/her main duties and responsibilities and where is necessary, assistant compliance officers
- Approval of the AML policy and procedures
- Communication of the AML policy to all employees of the Organisation
- Ensuring that the requirements of the Law and the AML Directive are applied, and that the Organisation maintains appropriate, effective and sufficient systems and controls for the prevention of money laundering and terrorist financing
- Ensuring that the Anti-Money Laundering Officer has full access to all documents and information necessary for the execution of his/her duties and responsibilities
- Ensuring that all employees of the Organisation know the Anti-Money Laundering Officer and report to him/her all suspicious transactions in accordance with the requirements of the AML Laws and the Directive
- Establishing a clear and quick reporting chain of suspicious transaction to the Anti-Money Laundering Officer
- Ensuring that the Anti-Money Laundering Officer has sufficient resources, staff and technology, for the effective execution of his/her duties and responsibilities
- Assessing and approving the Annual Report
- Reviewing the report submitted to the Board by the Anti-Money Laundering Officer

Since the overall responsibility for the prevention of money laundering and terrorist financing lies with the Board of Directors, they are also responsible for the assessment and approval of the Annual Report prepared by the Anti-Money Laundering Officer and for taking any necessary actions as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the Report.

3. INTERNAL AUDIT

3.1 The Organisation has assigned an Internal Auditor in order to continuously test current practices and inform the Organisation in case there are any suggestions for improvements. The Audit is performed at least on an annual basis.
Any findings are being submitted to the Board of Directors which decides the necessary measures that need to be taken to ensure the rectification of any weaknesses and/or deficiencies, which have been detected.

4. ROLE AND RESPONSIBILITIES OF AML OFFICER

4.1 The AML Officer has the necessary authority, resources and expertise to carry out his/her relevant duties and responsibilities and also has access to all relevant information. The employees of the Organization are informed of the person carrying out AML role and on ways of contacting him/her.

Currently, 1 employee has been assigned the role of AML Officer: Adrian Olivier Soto Lopez

In case of any changes in the structure of AML Department – this will be communicated to the Computer Gaming Licensing Board accordingly.

4.2 Responsibilities of AML Officer:

- To draft the Organisations' procedures and controls for the Prevention of the Money Laundering and Terrorism Financing
- To develop and improve Customer Acceptance Policy and submit it for approval of the Board of Directors
- To monitor and evaluate the sound and effective implementation of the Organization's general policy principles and to manage the associated risks in relation to the Prevention of Money Laundering and Terrorist Financing
- To ensure that KYC and EDD procedures are adhered to
- To ensure Sanctions Compliance procedures are adhered to
- To advise employees on issues arising as part of implementation of anti-money laundering program within the Organisation
- To provide necessary materials and trainings on AML/CTF and Sanctions Compliance to the employees of the Organisation
- To immediately inform the Board of Directors of any cases of non- compliance with laws, regulations and directives issued by the Governor
- To recommend to the Board of Directors any amendments necessary to the AML Policy
- To receive and evaluate information from all personnel regarding suspicious client transactions and activities
- If considered necessary – to report such transactions and activities to the Governor
- To ensure the preparation, maintenance and updating of lists of clients categorization following a risk-based approach.
- To screen existing clients and transactions to ensure that the AML policies are followed
- To detect, record and evaluate, at least on an annual basis, the risks arising from existing and new clients, new financial instruments and services and make any necessary amendments to the systems and procedures of the Organisation.
- To prepare and submit to the Computer Gaming Licensing Board the monthly prevention statement in a timely manner
- To Report to Senior Management, at least annually, on compliance issues indicating in particular whether appropriate remedial measures have been taken in the event of any deficiencies identified
- To prepare the Annual AML Report and submit it to the Board of the Directors

5. AML ANNUAL REPORT

5.1 The Annual Report, prepared by the AML Officer is a significant tool for assessing the Organisations level of compliance with its obligations as these are laid down in the Law and the Anti-Money Laundering Directive.

5.2 The Annual Report will be prepared and submitted for approval to the Board of Directors, within two months from the end of each calendar year (the latest by the end of February) and to the Governor, if requested, together with the minutes of the meeting, during which the Annual Report has been discussed and approved. It is provided that the said minutes will include the measures decided for the correction of any weaknesses and/or deficiencies identified in the Annual Report and the implementation timeframe of these measures.

5.3 The Annual Report should deal with money laundering and terrorist financing preventive issues pertaining to the year under review and, as a minimum, should cover the following:

- Information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the AML Directive which took place during the year under review
- Information on the inspections and reviews performed by the AML Compliance Officer, reporting the material deficiencies and weaknesses identified in the policy, practices, measures, procedures and controls that the Organisation applies for the prevention of money laundering and terrorist financing. In this regard, the report outlines the seriousness of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation
- The number of internal suspicion reports submitted by employees of the Organisation to the AML Compliance Officer, and possible comments/observations thereon.
- The number of reports submitted by the AML Compliance Officer to the Governor, with information/details on the main reasons for suspicion and highlights of any particular trends
- Information, details or observations regarding the communication with the employees on money laundering and terrorist financing preventive issues
- Information on the policy, measures, practices, procedures and controls applied by the Organisation in relation to high-risk clients as well as the number and country of origin of high-risk clients with whom a business relationship is established.
- Information on the procedures applied by the Organisation for the ongoing monitoring of client accounts and transactions
- Information on the training courses/seminars attended by the AML Compliance Officer and any other educational material received
- Information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organized, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and

specifying whether the course/seminars were developed in-house or by an external organisation or consultants

- Results of the assessment of the adequacy and effectiveness of staff training
- Information on the recommended next year's training program.
- Information on the structure and staffing of the department of the Compliance Officer as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

6. MANDATORY RISK PROCEDURES AND THE RISK-BASED APPROACH

6.1 General

The principle behind the Risk-Based Approach of the Company is that resources should be directed proportionately in accordance with the extent of the ML/FT risks posed, so that the customers posing the highest risks receive the highest attention meeting regulatory needs while effectively combating ML/FT. The application of a Risk-Based Approach should ensure that measures to prevent or mitigate ML/FT are commensurate with the risks identified and that resources are allocated in the most efficient ways.

The Policy sets the framework of the Company's Risk-Based Approach that should be implemented.

6.2 As regulation needs and risks always change, the AML Officer shall monitor and evaluate, on an on-going basis, the effectiveness of the measures and procedures of the adopted Risk–Based Approach. The AML Officer shall also be responsible for the development and implementation thereof, of all the other policies, procedures and controls according to the framework of the adopted Risk-Based Approach. The Board shall be responsible for reviewing the adequate implementation of the adopted Risk-based Approach by the AML Officer, at least annually.

Risk factors that must be taken into account, relating to:

- Client Category
- Jurisdiction
- Product/Service Type
- Transactions
- Distribution Channels

6.3 ADOPTED RISK-BASED APPROACH

The adopted Risk-Based Approach that is followed by the Organization, and described in the Policy, was built according to the following:

- recognising that the ML/TF threat varies across Clients, countries and financial transactions;

- allowing the Organisation to differentiate between Clients of the Organisation in a way that matches the risk of their particular profile and financial transactions;
- allowing the Organisation to apply its own approach in the formulation of policies, procedures and controls in response to the Organisations' particular circumstances and characteristics;
- helping to produce a more cost-effective system;
- promoting the prioritisation of effort and actions of the Organisation in response to the likelihood of ML/TF occurring through online gaming and betting transactions.

The Risk-Based Approach adopted by the Organisation, involves specific measures, indicators, and procedures in assessing the most cost effective and appropriate way to identify and manage the ML/TF risks faced by the Organisation. Such measures include:

- identifying and assessing the ML/TF risks emanating from profile particulars of Clients, amounts and particulars of deposits;
- managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls;
- continuous monitoring and improvements in the effective operation of the policies, procedures and controls;
- application of appropriate measures and the nature and extent of the procedures in line and as a result of different indicators. Such indicators include the following:
    - geographical spread of the transactions and Clients
    - the industry standard practices of providing online gaming and betting services
    - the volume and size of transactions
    - the country of origin and destination of Clients' funds
    - deviations from the anticipated volume of transactions
    - recording the action(s) taken so the Organisation shall be, at all times, in a position to demonstrate to the Computer Gaming Licensing Board or Governor that the extent of ML/TF measures and control procedures it applies are proportionate to the risk it faces while providing online gaming and betting services.

6.4 IDENTIFIED RISKS

The Risk-Based Approach adopted by the Organisation involves the identification, recording and evaluation of the risks that have to be managed. Whereas online gaming and betting services that the Organisation provides are rendered predominantly in straightforward manner: to relatively few Clients or Clients with similar characteristics - then the Organisation shall apply procedures enabling to focus on those Clients who fall outside the 'norm'.

The following are sources of risks which the Organisation faces with respect to ML/TF and respective risk categories the Organisation shall take into consideration when adopting a Risk-Based Approach and building Client ML/TF risk categorization:

Client's nature:

- PEPs
- Clients engaged in transactions which involve significant amounts of money
- Clients originating from high-risk countries or countries known for high level of corruption or organised crime or drug trafficking
- Clients reluctant to provide appropriate information
- Clients using VPN or Proxy servers to hide their IP addresses
- Clients using different devices to access the website of the Organisation

The Organisation's services:

- amount, origin and destination of funds for deposits and withdrawals
- deposit and withdrawal method
- nature of the online gaming and betting industry

6.5 ADOPTED RISK-BASED APPROACH

The adopted approach is considering that a risk assessment based on the above sources of risk should always be performed at the inception of a Business Relationship with a Client. However, a comprehensive risk profile may only become evident once the Client has begun transacting through an account and completed CDD procedure.

Taking into consideration the above and the fact that the Company will offer online gaming and betting facility and the fact that vast majority of its Clients will be applying on a non-face-to-face basis, following the performance of the CDD the Company shall label the type of Client and the risk profile (High risk, Medium risk, Low risk) according to the following different risk variables and indicators:

	Indicators related to the Client
High ML/TF Risk	PEPs Clients from countries that are selectively sanctioned resident or origin in/from non-reputable jurisdiction according to the FATF list as amended from time to time High Deposits any other Client determined by the Company itself to be classified as such Or any unverified client Any of the above-mentioned indicators will automatically classify the account as High Risk

Medium ML/TF Risk	Client that holds all of the below indicators: Verified client Client that does not fall under any of the categories of High Risk any other Client determined by the Company itself to be classified as such
Low ML/TF Risk	Client that holds all of the below indicators: Resident and origin of an EEA jurisdiction Very low deposits the country of origin and/or destination of Clients' funds are both EEA jurisdiction client using only debit/credit card or wire transfer clients identified Face-To-Face Or any Client who does not fall under the 'Medium Risk' or 'High Risk' categories

The methodology that is being adopted will require the AML Officer to perform basic CDD in cases of Low ML/TF cases, basic CDD and close monitoring in Medium risk cases, and EDD and close monitoring (on the specific indicator that increased the risk level) in cases of High Risk.

The intensity of monitoring all Clients' accounts and examining transactions shall be based on the level of risk and, as a minimum, shall achieve the ability of identifying all high risk Clients.

6.6 DYNAMIC RISK MANAGEMENT AND MONITORING

Risk assessment and management is not an isolated event of a limited duration but rather a continuous process, carried out on a dynamic basis. Clients' activities change, the same happens to the transactions used for money laundering or terrorist financing.

In this respect, it is the duty of the AML Officer to undertake regular reviews of the characteristics of existing Clients, new Clients, and the measures, procedures and controls designed to mitigate such risks. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

For the development and implementation of appropriate measures and procedures on a Risk-Based Approach, and for the implementation of the CDD, the AML Officer and the Client Support Department shall consult data, information and reports e.g. Clients with origin or residence in countries which inadequately apply Financial Action Task Force's (hereinafter "FATF"), and country assessment reports that are published in following relevant international listings:

- FATF
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures
- The EU Common Foreign & Security Policy (CFSP)

- The UN Security Council Sanctions Committees
- The International Money Laundering Information Network (IMOLIN)
- The International Monetary Fund (IMF)

Due to the nature of business of the Organisation, additional countries must be banned from the use of the services due to local and foreign gambling and betting regulations.

Additionally, the Organisation has implemented controls that monitor players activity and actions, that are unique to gambling and betting industries and are also a part of the fraud-prevention system, such as:

- use of VPN and Proxy Servers
- use of different devices to access services
- frequency of deposits
- payment methods used
- use of a variety of payment methods or sudden switch from one payment method to another
- attempts to use cards that did not pass 3D secure verification
- attempts to use cards with insufficient funds
- use of several bank cards
- attempt to withdraw funds through a payment method that has not been previously used
- Bet to deposit ratio
- Bet to current balance ratio

Such triggers may influence the overall risk assessment of the customer, as well as may lead to a submission of suspicious activity report or account termination.

7. SANCTIONS COMPLIANCE POLICY

7.1 The purpose of the Sanctions Compliance Policy is to set the high-level principles and standards of Qintara Limitada for the management and prevention of sanctions breaches and to establish an internal control framework that mitigates the risks associated with sanctions violations.

The Organisations compliance with sanctions regulatory framework is vital for:

- Avoidance of an administrative and/or regulatory action against the Organisation
- Protection of Organisations reputation

The recipients of the Policy are:

- AML Compliance Department
- Board of Directors
- Payments Department / Back Office

7.2 WHAT ARE SANCTIONS AND EMBARGOES

Sanctions and embargoes are political trade restrictions put in place against target countries with the aim of maintaining or restoring international peace and security.

Embargoes on exporting or supplying arms and associated equipment, technical assistance, trading and financing.

Financial sanctions on individuals in government, government bodies and associated companies, or terrorist groups and individuals associated with those groups.

Bans on imports of raw materials or goods to sanction countries/jurisdictions.

Restrictions on certain type of activities for certain entities subject to sectorial sanctions.

7.3 AUTHORITIES ISSUING SANCTION PROGRAMS

- OFAC (USA)
- EUROPEAN UNION
- UNITED NATIONS

7.4 TYPES OF SANCTIONS PROGRAMS

7.4.1 Specific/List based - relate to specific lists of named individuals, legal entities, organisations, vessels.

7.4.2 General – cover certain countries or jurisdictions and restrict a number of activities such as export of certain goods, products, dual-used items etc. that can be used for military purposes (e.g. steel, chemicals, arms sales to a particular country).

7.4.3 Comprehensive – cover all types of activities including business relationships and/or transactions connected with certain countries/jurisdictions subject to comprehensive sanctions (i.e. North Korea, Crimea).

7.4.4 Sectoral – cover certain entities (and their majority subsidiaries) engaged in specific sectors of the Russian economy and restrict certain activities of these entities that involve new “debt” or “equity” or drilling activities.

7.5 MEASURES APPLIED BY THE ORGANISATION FOR SANCTIONS COMPLIANCE

7.5.1. SANCTIONS RISK ASSESSMENT

The Organisation shall carry out and document a sanctions risk assessment appropriate to the type of its activities, in order to identify, measure, understand and manage sanctions risk the Organisation is exposed to. In assessing sanctions risk the Organisation shall take into account at least following factors that have an impact on sanctions risk:

- in relation to the activities of the Organisation:
    - a region where the Organisation operates and provides services, including the state where the Organisation's structure – subsidiary, branch, representation – operates and provides services;
    - services and products provided by the Organisation;

- in relation to the Organisation's customers, the Organisation takes into account circumstances affecting risk laid down in the Law on the Prevention of Money Laundering and Terrorism Financing:
    - customer risk,
    - risk of the state and geographical risk,
    - risks associated with services provided to customers and
    - service delivery channels, assessing them in the context of sanctions risk.

7.5.2 The Organisation shall carry out a sanctions risk assessment in relation to all sanctions and the sanctions risk assessment shall be approved by the Board of the Organisation.

7.5.3 Based on the sanctions risk assessment, the Organisation shall establish an internal control system for sanctions risk management. Sanctions risk policies shall be approved by the Board of Directors.

7.5.4 Establishing an internal control system for sanctions risk management the Organisation takes into account at least following characteristics of elevated sanctions risk:

- the customer, customer's transactions are related to a territory or border area of a territory or state that is a subject of sanctions;
- economic activity of the customer or if the customer is related to a military industry; sale, manufacture, import or export of dual-use goods subject to sectoral sanctions, or specialised foreign agencies (military design bureaux, space technology research agencies, etc.).
- the customer's economic or personal activities do not meet their declared economic or personal activities;
- the customer submits the same documents to justify several unrelated transactions;
- the documents supporting transactions submitted by the customer contain indications of fraud, providing evidence of possible evasion of sanctions;

7.6 KYC MEASURES ON NEW AND EXISTING CUSTOMERS FOR SANCTIONS COMPLIANCE PURPOSES

The Organisation has implemented relevant KYC and due diligence procedures that ensure that upon onboarding and throughout the business relationship, the relevant parties are being screened against sanction lists. In the event of a match, an alert will be generated for further investigation by the AML Compliance Department.

7.7 DUE DILIGENCE ON CUSTOMER TRANSACTIONS FOR SANCTIONS COMPLIANCE PURPOSES

The Organisation has implemented relevant procedures and processes that ensure that transaction parties (meaning, that the screening is performed not only against the Customer, but also against the payments institution) are being automatically screened against sanction lists. In the event of a match, an alert will be generated for further investigation by the AML Compliance Department.

7.8 IMPLEMENTATION OF AUTOMATED SANCTION SCREENING TOOL

Qintara Limitada has introduced an IT-based solution to fulfil the screening obligations automatically. All of the Organisation customers' key data (such as name, surname, and address) is automatically exported and matched with the sanctions lists. These checks are performed on a daily basis. The external service

provider is responsible for the actuality of sanctions lists on a daily basis and automatically performs regular checks of customers against the updated sanctions lists. If during the matching procedure a customer is marked as a potentially Restricted Party, this is defined as a match. This IT-solution simultaneously generates an alert message including all recorded matches, which is submitted to the AML Compliance Department. The automated IT solution performs:

- Daily automated screening of existing customers and on-going screening of transactions against prevailing sanction lists
- On-going monitoring of sanction programs administrated by the competent authorities in order to promptly implement the necessary measures and controls to ensure compliance with the sanctions programs

7.9 TESTING AND AUDIT OF AUTOMATED IT SOLUTION

It is the obligation of the AML Compliance Department to test the automated IT solution in order to ensure that the results received during screening are accurate and that the sanction lists are updated in a timely manner. The testing should be performed not less than every 6 months as well as at the point of introduction of new sanctions.

7.10 FREEZING AND UNFREEZING ACCOUNTS SUBJECT TO SANCTIONS

Where required by applicable law, the Organisation will freeze assets in accounts of parties subject to specific sanctions or where the freezing is otherwise indicated. The Sanctions Policy also requires freezing of accounts pending review to determine if an asset freeze is required or a violation of law has occurred.

The Organisation must freeze accounts of parties subject to specific sanctions as follows:

- Organisation must freeze accounts of parties where required under and E.U. laws;
- Organisation must freeze accounts for parties sanctioned under U.S. laws where U.S. jurisdiction applies.

Frozen accounts may be unfrozen only by:

- authorization from the jurisdiction which required the freezing, or
- an official removal of the specific sanctions leading to the asset freeze or blocking.

Organisation should not participate in transactions involving parties who are subject to specific sanctions implemented by EU, UN and “OFAC”, unless these transactions are allowed under the relevant sanctions, as confirmed in advance by the AML Compliance Department.

8. CLIENT ACCEPTANCE POLICY

8.1 The CAP will follow the principles and guidelines described in the Policy, and will define the criteria for accepting new Clients. This policy also defines the Client categorisation criteria which shall be followed by the Organization and especially by the employees which shall be involved in the Client account opening process.

The AML Officer shall be responsible for applying all the provisions of the CAP. In this respect, the Client Support Department shall also be assisting the AML Officer with the implementation of the CAP, as applicable.

The AML Officer shall review and evaluate the adequate implementation of the CAP and its relevant provisions, at least annually.

8.2 General Principles of the CAP

The Organization shall classify Clients into three various risk categories and based on the Risk-Based Approach described above.

- where the Client is a prospective Client, an account must be fully operational only after the relevant CDD and measures and procedures have been conducted, according to the principles and procedures set in the Policy.
- it shall be prohibited for persons engaged in the Company to open or maintain anonymous or numbered accounts or accounts in names other than those stated in the Client's official identity documents. No account shall be opened in anonymous or fictitious names(s).
- No account shall be made fully operational unless the Client's CDD is approved by the AML Officer.

8.3 Criteria for Accepting New Clients (based on their respective risk)

The Organization shall accept Clients who are categorised as Low Risk Clients as long as the Client passed a CDD and as long the general principles under the current Policies are followed.

The following list predetermines the type of Clients who are not acceptable for establishing a Business Relationship with the Organisation:

- Clients who fail or refuse to submit, the required data and information for the verification of their identity, without adequate justification
- Clients who ask to open or maintain anonymous or numbered accounts or accounts in names other than the client's name stated in official identity documents
- Client who ask to transfer its initial deposit in cash
- Legal entities
- Account opened in the name of a third person
- The documents submitted appear to be faulty at the examination stage
- The client comes from one of the non-cooperative jurisdictions
- The client has negative information/reports on him or is under investigation
- The client is on the list of people involved in terrorist financing or known to be involved in activity connected to money-laundering
- Sanctioned individuals

9. CLIENT DUE DILIGENCE, IDENTIFICATION AND VERIFICATION PROCEDURES

9.1 APPLYING CDD AND IDENTIFICATION PROCEDURES

The Company shall duly apply Client identification procedures and CDD measures in the following cases:

- when establishing a Business Relationship
- when there is a suspicion of ML/TF, regardless of the amount of the transaction
- when there are doubts about the veracity or adequacy of previously Client identification data
- when there are significant amounts deposited in the Players account
- any other event when the AML Officer finds it necessary

In this respect, it is the duty of the AML Officer to apply all the relevant procedures mentioned in this Policy.

Furthermore, the Customer Support Department shall also be responsible to collect and file the relevant Client identification documents, according to the record keeping procedures described in the Policy.

9.2 Further, the AML Officer shall be responsible to maintain at all times and use during the application of CDD and identification procedures with respect to required documents and data from potential Clients, as per the requirements of the Law and the Directive.

The AML Officer shall be responsible to review the adequate implementation of all the policies and procedures mentioned in the Policy, at least annually.

The Organisation commences the Business Relationship after it has duly performed at least the following actions:

- Identified the Customer and, within an allowed time limit, verified its identity by collecting identification documents
- Determined the purpose and intended nature of the Business Relationship
- Assessed the ML/TF risk of the Customer and allocated the Customer to an appropriate risk category in accordance with Procedure on Customers' risk assessment
- applied appropriate CDD or EDD measures
- Screened the relevant persons against the relevant financial sanctions list

In case, where the Organisation cannot comply with customer due diligence requirements, such as:

- to determine whether the Customer operates on their own behalf or is controlled;
- obtain the information about the purpose and intended nature of the Customer’s Business Relationship;
- verify the identity of the Customer according to the documents, data or information obtained from a reliable and independent source;
- conduct the ongoing monitoring of the Customer’s Business Relationship, transactions performed during the course of Business Relationship

- comply with the other requirement to apply the CDD or EDD measures,

it does not establish a business relationship and terminates the business relationship, and considers, if necessary, reporting the case to the Governor.

9.3 CUSTOMER IDENTIFICATION

The initial identification of the Customer is performed through the review of the initial registration of the players' account.

The registration collects the following information:

- Account number (generated automatically)
- Password
- Registration Date (generated automatically)
- Security Question
- Answer to Security Question (double input required)
- Phone number (must be verified)
- Email Address (must be verified)
- Surname
- First Name
- Date of Birth
- Type of Document
- Document Number
- Document Issue Date
- Country
- Permanent Registered Address

The following data allows the AML Department to perform their initial screening on the potential client.

9.4 VERIFICATION OF DOCUMENTS

The Organisation, when verifying the identity of the natural person the AML responsible employee must:

- review the documents provided for verification of the customer to ensure that no fraud signs have been noticed;
- ensure that document provided for identity verification is valid and contains the persons photograph;
- the Responsible employee must verify the data, documents, and information received from the Customer during the CDD using the documents, data or information obtained from a reliable and independent source.

9.5 STANDARD KYC AND CUSTOMER DUE DILIGENCE PROCEDURES

This section sets out the minimum and standard identification and due diligence measures that should be applied to customers.

The risk classification that will be attributed to the customer following the risk assessment and scoring, will determine the further due diligence measures that should be applied for each of these customers.

The true identity of natural persons should be ascertained by obtaining the following information:

- True name and/or names used as these are stated on:
- the official valid identity card (front and back) or the official valid passport, if the person in question is the national of a country within European Union; or
- the official valid passport, if the person in question is the national of country outside the European Union, which bears a photograph of the person
- full permanent address, including the postal code
- Telephone number
- E-mail address
- Date and place of birth
- Specimen signature (when obtaining the personal identification document)
- Information on public positions which the person holds or has held in the last twelve months or previously, as well as whether he/she is an immediate family member or close associate of a person who holds or has held in the last twelve months or previously a public position in order to determine whether the person is a PEP (should be obtained independently, through the screening database)

In addition to name verification, it is important that the permanent residential address of the customer is also verified by using one of the following means:

- Obtaining a recent (up to 3 months) utility bill issued on the name of the customer (e.g. electricity, water, gas, waste) or copy of municipal tax bill or a bank statement from a reputable Financial Institution
- Telephone bills of a landline only or internet bills (where a landline is required) could also be accepted.

9.6 In order to protect against forged or counterfeit documents, the prospective customers should be required to produce a copy of the original document (not online statements).

Note: the utility bills provided, should be reviewed, in order to ascertain that there has indeed been consumption of the service that the utility bill corresponds to, as a way to determine that the information declared by the customer is true. Evidence of consumption will be a strong indication that the address declared by the customer, is indeed the true current residential address.

The document evidencing the proof of residence and the copies of the passport/identity card pages containing all relevant information (at least passport's/ID's number, issuing and expiry date and country

as well as the customer's date of birth and a clear photograph of the documents owner and signature) should be kept in the customer's file.

9.7 In addition, further to the information to be provided by the person him/herself, a search should be made through the dedicated software and on the internet in order to obtain information on public positions which the prospective customer holds or held for at least the last twelve months or previously as well as whether he/she is an immediate family member or a close associate of such individual, in order to verify if the customer is a PEP.

10. ENHANCED IDENTIFICATION AND DUE DILIGENCE PROCEDURES FOR HIGH-RISK CUSTOMERS

10.1 The Organisation is required to take additional and enhanced measures in cases which by their nature, present a high-risk of money laundering and terrorist financing.
Apart from the Players accounts that have been classified by the Organisation as High-Risk, through its' risk assessment, the Laws and Directives additionally specify the below categories of customers which should be classified as high-risk and where enhanced due diligence measures should be applied:

- Complex and unusually large transactions or unusual types of transactions
- Accounts of PEP's
- Transactions with a natural person or legal entity established in a third country of high risk.

The minimum enhanced due diligence measures that should be applied for all High-Risk customers of the Organisation are:

- Perform review and update of records of the customer at least once a year or at a shorter interval if necessary
- Taking more enhanced measures and supporting documentation to establish and verify the source of wealth
- Perform systematic and thorough monitoring of the transactional behavior.

10.2 CUSTOMERS HAVING COMPLEX OR UNUSUALLY LARGE TRANSACTIONS OR UNUSUAL TYPE OF TRANSACTIONS

The Organisation is required to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions and all unusual types of transactions carried out without the apparent or legitimate purpose.

In order to further assess and determine whether such transactions or activities appear suspicious or not, the Organisation should classify the customer(s), engaging in such complex or unusually large or unusual transactions, as high-risk, in order to intensify the extent and nature of the monitoring of the business relationship.

Examples of complex or unusually large or unusual types of transactions include transactions that:

- Are not in line with those expected on the basis of the Organisation's knowledge of the customer and the business relationship or the category to which the customer belongs

- Constitute an unusual or unexpected type of transaction compared to the normal activity of the customer or the type of transactions associated with similar customers products or services, or
- Are particularly complex compared to other similar transactions related to similar items, products or customer services.

When the Organisation detects complex or unusually large or unusual types of transactions, and it was not informed of the relevant economic rationale or the legitimate purpose or has doubts as to the accuracy of the information received, the Organisation should apply enhanced due diligence measures on the particular client(s) involved in the transaction(s) and ascertain whether the specific transactions raise suspicion or not.

Such enhanced due diligence measures, include but are not limited to:

- Application of reasonable and adequate measures to understand the background and purpose of these transactions, e.g. by locating the source of the funds (by obtaining Bank statements, payslips or other documents that may provide relevant information) or by obtaining more information about the customer in order to determine the plausibility of the customer executing the specific transactions
- Intensify monitoring of the implied transactions and the customer's transactional history
- Monitoring of the business relationship on an annual basis, as provided for High-Risk customers in this procedure, or even more frequently if needed
- Assess whether the customer should continue to be classified as High Risk or further actions are needed.

The set of enhanced due diligence measures to be applied for each customer will depend on the circumstances of each individual case and the characteristics that rendered the transaction complex or unusual.

10.3 POLITICALLY EXPOSED PERSONS (PEPS)

The establishment of a business relationship with Politically Exposed Persons may expose the Organisation to increased risks, and it is considered one of the most important money laundering issues worldwide. The Organisation should be extra cautious when dealing with PEPs and as such they should be classified as High-Risk and enhanced due diligence measures should be applied. The Compliance department and other responsible employees should strictly comply with the provisions of the present Policy, regarding PEPs.

It should be stressed that the Organisation should be extra cautious when dealing with PEPs coming from High-Risk third countries facing widespread corruption problems and economic destabilization and that their standards of combating money laundering and terrorist financing are not equivalent to internationally accepted standards.

10.3.1 The Law defines Politically Exposed Persons as natural persons who have or had been entrusted with prominent public functions in the Republic or in a foreign country, as well as family members, or persons known to be close associates, of such persons.

10.3.1.1 For the purposes of this definition, "prominent public function" means any of the following public functions:

- Head of state, head of government, minister, deputy or assistant minister,
- Member of parliament or similar legislative body,
- Member of a governing body of a political party,
- Member of supreme court, a constitutional court or other high-level
- Judicial body whose decisions are not subject to further appeals, except in exceptional circumstances,
- Member of court of auditors and of the board of directors of Central Banks,
- Ambassador, charge d'affaires and high-ranking officer of the armed and security forces,
- Member of an administrative, management or supervisory body of a state-owned enterprises,
- Director, deputy director, director general of a Ministry and member of the board or equivalent function in an international organization,
- Mayor.

It is provided that none of the above-mentioned public functions shall be understood as covering middle-ranking or more junior officials.

10.3.1.2 "Family members" shall include the following persons:

- The spouse, or a person considered to be equivalent to a spouse of a Politically Exposed Person;
- The children and their spouses or persons considered. to be equivalent to a spouse of a Politically Exposed Person,
- The parents of a Politically Exposed Person.

10.3.1.3 "Close Associate" of a Politically Exposed Person" means a natural person:

- Who is known to have a joint beneficial ownership of a legal entity or legal arrangement or any other close business relation with a Politically Exposed Person,
- Who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a Politically Exposed Person.

It is provided that when a PEP has ceased to have a prominent public function in the Republic or in a Member State or in a third country or in an international organization, the Organization considers the business relationship as High-Risk, for a period of at least 12 additional months. The Organization assesses each case and maintains the PEP classification for as long as deemed necessary beyond the lapse of the 12 months, including for the whole future duration of the business relationship.
In the case of individual customers, where the applicant falls under the definition of a PEP, then the account should be classified a High-Risk - PEP.

10.3.2 In order to determine whether a prospective customer is a PEP, the Organization shall assess the below sources of information:

- Information provided by the person itself;

- The Screening data base; it is stressed, however, that the classification of a person as a PEP by Screening Data Base does not necessarily mean that the person is indeed a PEP. On the other hand, if a customer is not classified as a PEP by the Screening data base but information collected from other sources as per (i) above and (iii) or (iv) below qualify him/her as a PEP, then that person should be still classified as a PEP,
- Internet search,
- Any other reliable publicly available information.

10.3.3 Evidence for the search and the results from the above sources should be placed in the customer's file. The Organisation assesses each case and maintains the PEP classification for as long as deemed necessary beyond the lapse of the 12 months, including for the whole future duration of the business relationship if deemed appropriate.

10.3.4 If, upon the establishment of a business relationship, based on the above sources, a PEP is identified, and the business relationship is classified as PEP then the below additional enhanced due diligence measures should be followed:

- The decision for establishing a business relationship with a PEP or of continuing an existing business relationship where a PEP has been identified in the course of the business relationship, should be taken by the Board of Directors. The request for such an approval should be accompanied with a short report on the customer's profile and the PEP's profile prepared by the responsible employee, in order to obtain an informed decision from the Board of Directors.
- Before establishing a business relationship with a PEP, adequate information documentation should be obtained in order to ascertain not only the PEP's identity but also to assess their business reputation and/or integrity and/or professionalism (e.g. references from reliable third parties or internet searches that do not reveal concerns with reputation and/or integrity) if considered necessary,
- Adequate enhanced due diligence measures should be followed in order to establish the source of wealth and source of funds of the PEP that is involved in the business relationship in order to ensure that there are no funds originating from corruption or other criminal activity involved. The Organisation should focus on constructing the business / economic profile by obtaining the information/documentation as per the provisions of the present Policy. The source of wealth should be established based on the information provided through the communication with a potential PEP, which should be verified by documents.
- The regulatory framework emphasizes the importance of assessing particularly the sources of wealth of PEPs and requires the Organisation on a risk sensitive basis, to make every effort in order to verify the accuracy of the information provided by the PEP as to its wealth and the sources of this wealth against:
- Publicly available information sources such as asset and income disclosures which some countries expect certain public officials to file,
    - Publicly available property registers and/or land registers,
    - Company registers,

    - Internet searches including social media.
- The profile of the expected business activity should form the basis for the future monitoring of the relationship. The profile should be regularly reviewed and updated with new data and information. Particular caution should be given where the customer is involved in businesses which appear to be most vulnerable to corruption.
- All above information/documentation should be placed in the customer's file as evidence.

10.3.5 If upon the establishment of a business relationship, it is indicated on electronic databases that the applicant/ related individual is a PEP, however the Organisation has sufficient evidence to conclude that the individual in question has ceased to hold the public prominent position or in any other way does no longer fall under the definition of PEPs provided above, and should thus not be classified as High Risk - PEP, then this should be clearly evidenced in the customer's file. The customers file should include a note, adequately explaining the reason why it is the Organisation's position that the individual does no longer fall under the PEP definition - in contrary to what it is potentially stated in electronic databases - and make reference to the online or other sources that justify this decision. Evidence/ copies of these sources (e.g. articles, websites, newspaper extracts, evidence provided by reliable third parties and others) should be placed in the file. The above should also apply to cases where electronic databases do not classify an individual as PEP, however the Organisation has adequate evidence to conclude that the individual falls under the PEP definition and should thus be classified as PEP. Again, sufficient explanation should be added in the short note prepared for PEPs, as provided above in this section of the Policy, explicit reference should be made to the sources that the Organisation relied on in order to reach this conclusion, and sufficiently document everything in the file. The same approach should be also applied upon the review/ updating of the customer's file.
The above measures also apply for already established business relationships, where any of the natural persons involved becomes a PEP at any point throughout the business relationship. Such change in the customer's categorization should also take place if the screening system is not updated but this information is identified at any given time (e.g. during the review of any customer', where the natural person itself may inform the Organisation, etc.).

10.3.6 Business relationships with PEPs should be subject to enhanced and on-going monitoring. The Organisation should perform on-going monitoring on both the transactions and the risk profile of the customer:

- The review of the business relationship should be performed at least on an annual basis. The continuation of the business relationship should be approved by the Board of Directors. The thorough review of the transactional activity, as well as of the profile of the customer and the PEPs involved should be carried out by the AML Officer and the results of the review should be summarized on a short report. If, following the review, the AML Officer is satisfied that the business relationship should continue, the short report should accompany the request for continuation of the business relationship to the Board of Directors.
- The report should include, as a minimum:
    - Basic details such as date of establishing the relationship, whether the relationship is dormant, etc.

    - A comment on the actual turnover of the players account and whether it is in line with the expected turnover of the account (the conclusions on the expected turnover, should be formed on the documented source of funds and source of wealth that has been confirmed by documents).
    - A reference to connected/affiliated customers of the Organisation.
    - An express statement whether there is any suspicion for irregular activity of the client.
    - Clear recommendation to the Board of Directors for the continuation of the relationship or closure.
- During the ongoing monitoring of the transactions, the Organisation should be cautious in order to identify and pay particular attention to transactions that seem unusual/ out of the normal. Such transactions should be assessed based on the information maintained about the customer and the established business profile, and consider whether, in the light of the unusual transaction, the information maintained should be re- assessed and updated.
- If during the above review, or ongoing monitoring of the business relationship and transactions any suspicions are raised, the provisions of the relevant section of the present Policy should be followed.
- All documents concerning the renewal and the review should be placed together in the file.

10.4 CUSTOMERS RELATED TO OR TRANSACTING WITH THIRD COUNTRIES OF HIGH RISK

The Organisation classifies as High-Risk and applies enhanced due diligence measures, on customers physical persons who are nationals or residents of High-Risk countries.

The Law defines as a High-Risk third country, a country indicated by the European Commission which presents strategic deficiencies in its national system for combating money laundering and terrorist financing which are considered as major threats to the financial system of the EU.

Additionally, countries and geographic areas is one of the risk factors that the Organisation, should consider when identifying and assessing risks of money laundering and terrorist financing.

Taking into consideration the "Geographic Risk Factors" for the assessment and classification of a third country as High-Risk, as well as a number of lists and statements of European and international organisations, the Organisation has developed a Country Risk Categorization Methodology (hereinafter the "Methodology) on the classification of a third country as High risk, and how related customers and transactions shall be treated.

Based on the developed Methodology, the Organisation's list of High-Risk countries, includes inter alia jurisdictions which are:

- Subject to Sanctions/ Embargoes,
- Non-cooperative for tax purposes (EU list),
- FATF countries that bear deficiencies in their system of money laundering and terrorist financing,
- Under High Level of corruption, transparency, bribery etc.

It is the AML Compliance Department's responsibility to maintain and update the list of High-Risk countries, resulting from the Methodology and to communicate it to the Board of Directors and any other responsible employees when updated and amended.

The responsible employees should refer to the Methodology, as a guidance on how each category of High-Risk affects the customers and their transactions related to the country category.
For such customers and transactions, it is important to apply the enhanced due diligence measures especially regarding the establishment of the source of wealth, as per the provisions of the present Policy and the Organisation's Risk Assessment Policy.

10.4.1 In addition:

- Customers with transfers to and from High-Risk countries should be automatically classified as High-Risk. However, a margin of deviation from this rule may apply, on a risk-based approach, based on qualitative criteria and the nature of the transaction. For example, low risk and normal risk customers who may carry out a single transaction or rare payments of small amount to one of these countries, may be acceptable without reclassification of the customer to High-Risk.
- Transactions with persons from the afore-mentioned countries with no apparent economic or visible lawful purpose should be examined with the aim of ascertaining their financial, purpose. If, as a result, it is considered that the Organisation cannot satisfy itself as to the legitimacy of the transaction, this should form a ground for suspicion and the relevant provisions of this Policy should be followed.

10.5 SCREENING DATABASE

The Screening database comprises names of natural and legal persons, countries, organizations, vessels etc., which may, inter alia, be:

- Subject to sanctions
- Suspects for money laundering and terrorist financing activities,
- Politically Exposed Persons.

Apart from the above, it provides information of general nature on the persons included in the data base such as positions held currently and, in the past, possible negative information regarding accusations against them of any nature such as for tax evasion, for legal litigations, for relationship with PEPs or criminals, etc.
It must be noted that the Screening database check must be performed, and any discarded hits (false positives) should be assessed, explained, and included in the customer's file.
In case of true matches, these must be escalated to AML Department.
The database should be used screens the names of all active customers daily.

10.6 INTERNET SEARCH / MEDIA CHECK

Internet / media searches should always be performed on new applications and upon the review (either regular or ad hoc) of identification records or annual account review, for all clients and their relevant persons.
The internet search serves the purpose of identifying adverse media, obtaining as much information as possible in constructing the customer's profile, identifying whether the customer is a PEP or immediate

family member or close associate of a PEP as well as of cross-checking the information provided by the customer.
In evidencing the search, the officer preparing the customer's file should add and sign the following confirmation on the conciliatory page: "Internet search has been made". Search results should be assessed and copies to be kept in the customer files. It is reminded that where there are negative articles or public allegations on the customer or its officials, all the public information identified should be disclosed and outlined clearly in the Customers file and an assessment made as to the actions needed by the Organisation (e.g. reclassification to High-Risk, close monitoring, termination, etc.). The assessment in such cases must be discussed for final decision with the AML Officer.
Confirming that an "Internet search has been made" and failing to disclose easily available negative information for further assessment is a direct breach of the provisions of this Policy and may lead to the Organisation not fulfilling effectively its AML obligations.

11. ON-GOING MONITORING PROCESS

11.1 The constant monitoring of the Players' accounts and transactions is an imperative element in the effective controlling of the risk of ML/TF.
In this respect, the AML Officer shall be responsible for maintaining as well as developing the on-going monitoring process of the Organisation and use the appropriate IT systems in order to achieve highest monitoring abilities while keeping a cost-effective process.
The AML Officer shall review the Organisations' procedures with respect to the on-going monitoring process, at least annually.
The procedures and intensity of monitoring Clients' accounts and examining transactions on the Client's level of risk shall include the identification transactions which, as of their nature, may be associated with ML/TF, unusual or suspicious transactions that are inconsistent with the profile of the Client for the purposes of further investigation.

11.2 In case of any unusual or suspicious transactions, the head of the Client Support Department shall be responsible to communicate with the AML Officer.
Further to the investigation of unusual or suspicious transactions by the AML Officer, the results of the investigations are recorded in a separate memo and kept in the file of the Clients concerned the ascertainment of the source and origin of the funds credited to accounts.
Established minimum triggers, that would require an ongoing monitoring and request of additional documents:

- Cumulative deposits over 5000 EUR in 1 month
- Sudden increase in deposits
- High loss amount
- Deposits coming from different payment systems
- Request for withdrawals through an alternative payment system, different from the deposit method

11.3 It should be noted that these triggers are only samples of possible scenarios and each case should be treated on an individual basis, taking into consideration players transaction history, activity, previously obtained documentation and risk categorization.
The Organisation maintains relevant controls in order to track Players deposits and withdrawals, as well as have all the required technical requirements in order to review Players' transaction activity starting from the account opening. The data can be segregated in periods or types of transactions.

12. REVIEW AND UPDATING OF CDD

12.1 It is a requirement that the customers identification records should be examined on a regular basis so that it is ensured that they remain completely updated. In this respect, the procedures described below should be followed.

12.2 Regular review and updating

The frequency of review and updating depends on the risk categorization of each customer and should be as follows:

- **Low risk customers:** Not less frequently than once every 3 years,
- **Normal risk customers:** Not less frequently than once every 1 years,
- **High risk customers:** Not less frequently than every 6 months.

During the review procedure, the customer should be requested to confirm that the identification information held by the Organisation is still accurate and valid or advise changes that have taken place. In case that any change has taken place, the customer should be asked to present the relative supporting documentation / evidence.

12.3 It is pointed out that during the review process, new documents evidencing the permanent residential address of all natural persons should be obtained.
The Responsible employee is required to send the letter with the requirements for the update of information and records, reminders and the warning letter where needed and follow-up completion of the review procedure.
Completion of the review procedure should be approved by the AML Officer in the same way as for the establishment of a business relationship.
The continuation of the business relationship with High-Risk customers should be approved by the AML Department and in some cases, by the Board of Directors (e.g. PEPs).

13. TERMINATION OF THE BUSINESS RELATIONSHIP

13.1 The Organization should proceed with the termination of the relationship with an existing customer who:

- Had such changes in its status after the establishment of the relationship which turned it to be one of the prohibited types of customers as per the Customer Acceptance Policy,

- Has a behaviour in its transactions and activities which makes it a customer of excessive high-risk,
- Refuses or fails to provide updated information requested by the Organisation,
- Has attempted to deceive the Organisation,
- Breached any of the provisions of the Organisation's Terms and Conditions that the Organisation deems of significance,
- Has been convicted for any serious predicate offence, for which a Court Order or enquiry from an authority has been received and by maintaining the relationship may expose the Organisation to high AML or reputational risk,

13.2 Before proceeding with the termination of a business relationship, the Organisation should make sure that the files of the customer are KYC compliant and that the records are up to date. In this respect:

- When a customer requests to proceed with the termination, or where the Organisation wishes to proceed with the termination of the business relationship with a customer, the Organisation should be satisfied that the data and profile information of the customer are up to date. If not, the Organisation should carry out any necessary actions - depending on the case - to ensure that the customer's status and records become updated, and that there are no concerns obstructing the Organisation from proceeding with the termination.

- The Organisation shall not immediately proceed with the termination in cases where a customer's review and updating of records has not been completed. When review (either annual or ad-hoc) and updating of records is requested by the Organisation, and the customer does not provide all the necessary information for its completion this should constitute a ground of suspicion and it should be considered, whether it requires reporting to the Governor. Such cases should be treated, depending on the individual circumstances of each case. For example, if the Organisation can establish and be satisfied that, based on the circumstances and the customer's behaviour/attitude, not providing the required documentation does not raise any suspicions, then the Organisation may proceed with the termination. Evidence of such justification should be placed in the customers' file.

14. RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS / ACTIVITIES TO THE UNIT

14.1 REPORTING SUSPICIOUS TRANSACTIONS

Whenever there is an attempt of executing transactions that raise reasonable suspicion of being related to ML/TF, the AML Officer, reports the case to the Governor through the dedicated GoAML Portal in accordance with the current Policy.

14.2 SUSPICIOUS TRANSACTIONS

14.2.1 The definition of a suspicious transaction as well as the types of transactions indicating ML/TF is very broad. A suspicious transaction will often be inconsistent with the normal Business Relationship

patterns of the specific account. The Company shall ensure that it maintains adequate information and knows enough about its Clients' activities in order to recognise on time that a transaction or a series of transactions is unusual or suspicious.

Examples of what might constitute suspicious transactions/activities related to ML/TF are listed in Appendix 1 of the Policy. The relevant list is not exhaustive, nor it includes all types of transactions that may be used. Nevertheless, it can assist and serve as guidance to the Company and its employees (especially the AML Officer and the Client Support Department) in recognising the main methods used for ML/TF. The detection by the Company of any such 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 and the circumstances surrounding the particular activity.

14.2.2 In order to identify suspicious transactions, the AML Officer shall perform the following activities:

- monitor on a continuous basis any changes in the Players' transaction patterns
- monitor on a continuous basis if a Player is engaged in any of the practices mentioned in Appendix 1 of this Policy.

Furthermore, the AML Officer shall perform the following activities:

- receive and investigate information from the Organisations' employees, on suspicious transactions which raises reasonable suspicion of ML/TF. This information is reported on the Internal Suspicion Report. The said reports are archived by the AML Officer
- if, as a result of the evaluation, the AML Officer decides to disclose this information to the Governor, then a report is submitted to the Governor
- if as a result of the evaluation described above, the AML Officer decides not to disclose the relevant information to the Governor, then he/she fully explains the reasons for his decision on the Internal Evaluation Report

14.3 AML OFFICERS' REPORT TO THE UNIT

14.3.1 All the reports of the AML Officer will be send or submitted directly to the Governor.

After the submission of a suspicious report according to the Policy, the Organisation may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Organisation exercises particular caution in order not to alert the Client concerned that a suspicious report has been submitted to the Governor. Close liaison with the Governor is, therefore, maintained in an effort to avoid any impediment to the investigations conducted.

14.3.2 After submitting the suspicious report, the Organisation adheres to any instructions given by the Governor and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

The Governor may instruct the Organisation to refrain from executing or delay the execution of a Client's transaction without such action constituting a violation of any contractual or other obligation of the Organisation and its employees.

14.3.3 Furthermore, after the submission of a suspicious report according with the current Policy, the Clients' accounts concerned as well as any other connected accounts are placed under the close monitoring of the AML Officer.

14.4 SUBMISSION OF INFORMATION TO THE UNIT

The Company shall ensure that in the case of a suspicious transaction investigation by the Governor, the AML Officer will be able to provide without delay the following information:

- the identity of the account holders
- data of the volume of funds or level of transactions flowing through the account
- accounts detected in similar behaviour
- in relation to specific transactions:
    - the origin of the funds
    - the type and amount of the currency involved in the transaction
    - the form in which the funds were placed or withdrawn
    - the identity of the person that gave the order for the transaction
    - the destination of the funds
    - the form of instructions and authorisation that have been given
    - the type and identifying number of any account involved in the transaction

15. RECORD-KEEPING PROCEDURES

15.1 PURPOSE OF KEEPING RECORDS

The Organisation shall retain records, including documentation and information, for use in an investigation into, or an analysis of, the possibility of ML/FT. These records can be requested by the Computer Gaming Licensing Board Anjouan or the Governor or by other relevant competent authorities as required. The records maintained by the Organisation are extremely important to competent authorities responsible for analysis, investigation, law enforcement and prosecution since they may constitute evidence of the audit trail and of money flows. It is therefore crucial that subject persons adhere to the legal obligations applicable in this area.

In case the Organisation will establish a documents/data retention policy, the AML Officer shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive.

The AML Officer shall review the adherence of the Company to the above, at least annually.

15.2 RECORDS TO BE RETAINED

The Client Support Department of the Organisation shall maintain records of all documents related to the verification process performed on a client in relation to all Business Relationships formed:

- the Client identification documents obtained during the CDD, as applicable
- monitoring reports obtained during and after the establishment of Business Relationship

The Organisation should also retain the following records required as evidence of compliance with the Law and Directive and for statistical purposes:

- internal suspicious reports made to the AML Officer
- reports made by the subject person to the Governor
- a record of the reasons for not forwarding an internal report to the Governor
- a record of AML Officer training provided, including: the date on which the training was delivered; the nature of the training; the names of employees receiving the training; the results of any assessment undertaken by employees; a copy of any hand-outs or slides;
- other important records, including: any reports by the AML Officer to senior management/ Board of Directors made for the purposes of complying with the obligations under the Law.

15.3 PERIOD OF RETENTION OF RECORDS

The Organisation shall maintain the records for a period of at least five (5) years. The date of commencement of this time period depends on the type of records to be retained.

With respect to CDD and/or EDD documentation, the time period of five (5) years commences from the date on which the Business Relationship is terminated.

It is provided that the documents/data mentioned above which may be relevant to ongoing investigations shall be kept by the Organisation until the Governor confirms that the investigation has been completed and the case has been closed.

15.4 FORM OF RECORDS

The Organisation maintains records in any one of the following forms: physical file, scanned form, computerised or electronic form.

Subject persons should use a standardised approach to record keeping and must ensure that the approach used enables the quick retrieval of records for the purposes laid out in Section 15.4 below.

15.5 RETRIEVAL OF RECORDS

Subject persons are required to maintain efficient record-keeping procedures that enable them to retrieve information in a timely manner when so requested by the relevant authorities acting in accordance with the Law and Directive.

To this effect, the Organisation shall establish effective systems which are commensurate with the size and nature of its business and that enable it to respond efficiently, adequately, promptly and comprehensively to such enquires made to them by Computer Gaming Licensing Board, the Governor or other relevant competent authorities in accordance with Law. The provision of this information is of particular importance in the context of procedures leading to measures such as freezing or seizing of assets, including terrorist assets.

When requests for information are made by the Computer Gaming Licensing Board or the Governor, the Organisation should ensure that it is able to reply to these enquiries in a timely manner but not later than five (5) working days from when the demand is made, unless the subject person makes representations justifying why the requested information cannot be submitted within the said time.

15.6 CERTIFICATION & LANGUAGE OF DOCUMENTS

The documents/data obtained, shall be in their original form or in a copy form. A translation shall be attached in the case that the documents above are in a language other than English.

Each time the Company shall proceed with the acceptance of a new Client, the Client Support Department shall be responsible for ensuring compliance with the provisions of points above.

16. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING ON ANTI-MONEY LAUNDERING AND TF

16.1 The Organisations' employees can be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing.

The employees cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing.

The employees are aware of their obligations of not tipping off customers, where there are any suspicions in regard to money laundering or when there is an ongoing investigation.

16.2 The Organisation will organize internal and external training for its employees and AML Officer. The AML Officer will additionally provide training to the employees of the Organisation, when needed. The main purpose of the training is to ensure that relevant employees become aware of:

- the Anjouan Money Laundering (Prevention) Act 008 of 2005
- the European Union laws and directives
- the Organisations' Anti-Money Laundering Policy and relevant Procedures
- the statutory obligations of the Organisation to report suspicious transactions
- the employees own personal obligation to refrain from activity that would result in ML/TF

- the importance of the Clients' due diligence and identification measures requirements for ML/TF prevention purposes.

The training program will have a different structure for new employees and existing employees. On-going 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.

The Organisation will keep documented records, in regard to the trainings attended, dates and the names of the employees that have received the training.

17. REVIEW AND UPDATE OF THE POLICY

The adequacy of internal control measures intended for the prevention of money-laundering and terrorist financing shall be regularly revised in order to ensure that the measures implemented remain up-to-date and are proportionate to risks arising for the Organisation. The AML Policy must be reviewed at least annually as well as in the event of any changes in the applicable regulations and/or in cases when provision of new services are being considered.

Appendix 1

EXAMPLES OF SUSPICIOUS TRANSACTIONS/ACTIVITIES RELATED TO

MONEY LAUNDERING AND TERRORIST FINANCING

- The transactions or the size of the transactions requested by the Client do not comply with his usual practice and activity.
- Large volume of transactions.
- The Business Relationship involves only one transaction, or it has a short duration.
- Any transaction the nature, size or frequency appear to be unusual.
- Instructions of payment to a third person.
- Transfer of funds to and from countries or geographical areas which do not apply, or they apply inadequately FATF's recommendations on Money Laundering and Terrorist Financing.
- A Client is reluctant to provide complete information when establishes a Business Relationship.
- A Client provides unusual or suspicious identification documents that cannot be readily verified.
- A Client's home/mobile telephone is disconnected.
- Unexplained inconsistencies arising during the process of identifying and verifying the Client (e.g. previous or current country of residence, country of issue of the passport, documents furnished to confirm name, address and date of birth etc).
- Attempts to deposit funds through one payment system, but arranging the withdrawal of funds through another
- Receiving alerts from PSPs that the credit/debit card is lost/stolen/frozen

Appendix 2

Prohibited countries list:

Cuba, Iran, North Korea, Syria, Ukraine (Crimea, Donetsk, Luhansk), Russian Federation, Burma, Côte d'Ivoire, Congo, Eritrea, Iraq, Lebanon, Liberia, Libya, Somalia, Afghanistan, Burma (Myanmar), Central African Republic, Congo, Ethiopia, Sudan, Venezuela, Yemen, Zimbabwe, Australia, Austria, Belgium, Belize, Bulgaria, Colombia, Comoros, Croatia, Curacao, Denmark, Estonia, Finland, France, Georgia, Germany, Italy, Netherlands, Panama, Portugal, Romania, Spain, Sri Lanka, United Kingdom, United States, Aruba, Bonaire, Saba, Statia, St. Martin.