

Anti-Money Laundering Operations & Procedures Manual

WIN PRO GAMES B.V.

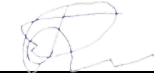
DATE: 2024-09-01

VERSION: 1.1

Document Information

Subject	Anti-Money Laundering Operations & Procedures Manual
Responsibility	Hanna Mykhailova, MLCO
Approval	Serhii Horbach, Executive Director
Classification	Internal Policy Document

Version Control

Version	Approval Date	Author	Change Status	Approved by	Signature
1.1	01.09.2024	Hanna Mykhailova, MLCO		Serhii Horbach Executive Director	

<u>Document Information</u>	2
<u>Version Control</u>	2
<u>1. DEFINITIONS</u>	5
<u>2. INTRODUCTION</u>	6
<u>2.1 Purpose</u>	7
<u>2.2 Definition of Money Laundering</u>	7
<u>2.3 Definition of Terrorism Financing</u>	8
<u>2.4 Definition of Financing of Proliferation of weapons</u>	8
<u>2.5 Applicability</u>	8
<u>2.6 Supervisory Authorities</u>	8
<u>2.7 Obligation perform Due Diligence measures as part of the Client Acceptance Process</u>	8
<u>3. CLIENT ACCEPTANCE POLICY (CAP)</u>	9
<u>4. RESPONSIBILITIES OF THE BOARD OF DIRECTORS</u>	9
<u>5. MONEY LAUNDERING COMPLIANCE OFFICER (MLCO)</u>	10
<u>6. RISK BASED APPROACH</u>	11
<u>6.1 General</u>	11
<u>6.2 Risk factors specific to the Gambling Sector</u>	11
<u>6.2.1 Customer risk</u>	12
<u>6.2.2 Product, service and transaction risk</u>	12
<u>6.2.3. Distribution channels risk</u>	13
<u>6.2.4. Geographical risk</u>	13
<u>6.3 Technological developments risk assessment</u>	14
<u>7. BUSINASS RISK ASSESSMENT (BRA)</u>	14
<u>7.1 Assessment of the Business Risk Assessment</u>	14
<u>7.2 Money transfers to third parties</u>	14
<u>7.3 Internal Investigations</u>	15
<u>7.4 Escalation and reporting to the Financial Intelligence Unit Curaçao (FIU)</u>	15
<u>7.5. Tipping-off</u>	15
<u>7.6 Updating the Internal Control Procedures</u>	15
<u>8. CLIENT DUE DILIGENCE</u>	15
<u>8.1 Scope of Application</u>	15
<u>8.2 Know your Client Principle (KYC)</u>	16
<u>8.3 Due Diligence Procedures</u>	16
<u>8.4 Reliance on Third Parties for Client Identification</u>	16
<u>9. SIMPLIFIED DUE DILIGENCE</u>	17
<u>9.1 Scope of Application</u>	17
<u>10. ENHANCED DUE DILIGENCE</u>	17
<u>10.1 Scope of Application</u>	17
<u>10.2 Enhanced Due Diligence Procedures</u>	18
<u>(a) Politically Exposed Persons</u>	18
<u>(b) Residents of higher risk geographic areas:</u>	18
<u>(c) Products or transactions that might favor anonymity:</u>	19
<u>(d) 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</u>	19
<u>10.3 The termination of the business relationship</u>	19
<u>11. ONGOING MONITORING</u>	20
<u>11.1 General</u>	20
<u>11.2 Ongoing monitoring</u>	20
<u>11.3 Ongoing Transaction monitoring</u>	20
<u>11.4 Ongoing monitoring of key risk factors</u>	20
<u>11.5 Timing of CDD Measures</u>	21
<u>11.6 Reliance on third parties to perform customer due diligence</u>	21
<u>12. TERMINATION OF BUSINESS RELATIONSHIP AND PROHIBITION OF DISCLOSURE</u>	21
<u>13. RECORD KEEPING</u>	22
<u>14. TRAINING OF EMPLOYEES</u>	23
<u>ANNEX I – CLIENT ACCEPTANCE POLICY</u>	24
<u>1. Introduction</u>	24

<u>2. General Principles of the Client Acceptance Policy</u>	24
<u>3. Prohibited Clients and Transactions</u>	24
<u>4. High Risk Clients</u>	25
<u>5. Client Approval Process</u>	25
<u>6. Identification requirements and verification procedures of a physical person</u>	25
<u>(a) Non-face to face identification procedures</u>	26
<u>(1) Uploading the photo of an ID document</u>	26
<u>(2) Checking the image for authenticity</u>	26
<u>(3) Checking image integrity</u>	27
<u>(4) Document data validation</u>	27
<u>7. Supported Identification Documents</u>	27
<u>8. Proof of address verification</u>	34
<u>(a) Non-face to face procedures</u>	34
<u>(b) Supported PoA Documents</u>	34
<u>9. Payment card verification</u>	36
<u>10. Liveness Detection</u>	36
<u>11. Source of Funds (SoF) and Source of Wealth (SoW)</u>	36
<u>ANNEX II - INDICATIONS OF AN UNUSUAL TRANSACTIONS</u>	38
<u>ANNEX III - "INTERNAL SUSPICION REPORT"</u>	39
<u>ANNEX IV - "INTERNAL EVALUATION REPORT"</u>	40
<u>ANNEX V – SANCTIONS POLICY</u>	41
<u>1. Background</u>	41
<u>2. Policy Statement</u>	41
<u>3. Sanction Screening</u>	42
<u>4. Asset Freezing</u>	43
<u>5. Outsourcing</u>	43
<u>6. Record-Keeping And Record Retention</u>	43
<u>ANNEX VI - REGISTRY OF TERMINATED TRANSACTIONS AND/OR THE BUSINESS RELATIONSHIPS</u>	44
<u>ANNEX VII – Country (Excell form)</u>	44

1. DEFINITIONS

- 1.1. **“AML”** means Anti-Money Laundering.
- 1.2. **“AML Manual”** means this “Anti-Money Laundering Operations & Procedures Manual” and all its annexes as amended from time to time.
- 1.3. **“AML Law”** means the “Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction”
- 1.4. **“Beneficial owner”** means a natural person who ultimately owns or controls the Client or a natural person on whose behalf a transaction is being conducted or monetary operations are being executed. The Beneficial owner shall include:
- 1) in the case of a legal person:
 - a) the natural person who owns or manages the legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights in that legal person, including through bearer shareholdings, or through control via other means, other than public limited liability companies whose securities are traded on regulated markets that are subject to disclosure requirements consistent with the European Union legislation or subject to equivalent international standards. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the Client held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the Client held by an undertaking, which is under the control of a natural person(s), or by multiple undertakings, which are under the control of the same natural person(s), shall be an indication of indirect ownership;
 - b) if no person under point (a) above is identified, or if there is any doubt that the person identified is the beneficial owner, the natural person who holds the position of senior managing official in the legal person who has been identified;
 - 2) in the case of a trust, all following persons:
 - a) the settlor/settlers;
 - b) the trustee/trustees;
 - c) the protector/protectors, if any;
 - d) the natural persons benefiting from the legal person or entity not having legal personality, or where such persons have yet to be determined, persons in whose main interest that legal person or entity not having legal personality is set up or operates;
 - e) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;
 - 3) in the case of a legal person which administers and distributes funds, an entity similar to a trust – the natural person holding an equivalent position to that referred to in point 2 above.
- 1.5. **“Business relationship”** means a business, professional or commercial relationship of the Company with a Client that is expected, at the time when entering in such a relationship, to have an element of duration.
- 1.6. **“Company”** means the company **Win Pro Games B.V.** with registration number 164220 with the registered address Abraham Mendez Chumaceiro Boulevard 03, P.O. Box 4750, Curacao. **Win Pro Games B.V.** (hereinafter – the “Company”) is a global digital agency and igaming operator, acting according to the laws of Curacao.
- 1.7. **“Client”** means a person that receives the services provided by the Company.

- 1.8. **“Employee of the Company”** or **“Employee”** means any natural person who is employed by the Company on the basis of employment agreement or other agreement that gives rise to an employer-employee relationship based on the facts and circumstances of the relationship.
- 1.9. **“Family member”** means spouse, person in registered partnership (cohabitant), parent, brother, sister, child and child’s spouse or child’s cohabitant.
- 1.10. **“Financial Transaction”** means in casinos these include the purchase or cashing in of casino chips or tokens, the opening of an account, wire transfers and currency exchanges. Financial transactions do not refer to gambling transactions that include only casino chips or tokens
- 1.11. **“FIU”** means The Financial Intelligence Unit Curaçao, referred to in art. 2 of the NORUT
- 1.12. **“Monetary operation”** shall mean any payment, transfer or receipt of money.
- 1.13. **“Money laundering”** or **“ML”** means the process used to conceal or disguise the nature, location, source, ownership or control of money or assets, obtained through criminal activity.
- 1.14. **“Money Laundering Compliance Officer”** or **“MLCO”** means an employee or appointed officer of the Company who is appointed by the Board of Directors of the Company as the officer responsible for the money laundering and terrorist financing prevention activities of the Company.
- 1.15. **“Suspicious Monetary operation or Transaction”** means a monetary operation or transaction relating to property which is suspected of being, directly or indirectly, derived from a criminal act or from involvement in such an act and/or is, as suspected, associated with terrorist financing.
- 1.16. **“Terrorist financing”** or **“TF”** means any act which constitutes an offence within the meaning of Article 2 of the International Convention for the Suppression of the Financing of Terrorism of 9 December 1999.

2. INTRODUCTION

This Anti-Money Laundering Operations & Procedures Manual (hereinafter the “AML Manual”) has been developed and is periodically updated by the Money Laundering Compliance Officer (hereinafter the “MLCO”) of **Win Pro Games** (hereinafter the “Company”) according to the applicable legal framework and based on the general principles as defined by the Company’s Board of Directors (hereinafter the “Board”) in relation to the prevention of money laundering and terrorist financing activities.

The Board of Directors of the Company is required to approve any amendments of this Anti-Money Laundering Operations & Procedures Manual.

The AML Manual shall be communicated by the MCLO to all the employees of the Company that manage, monitor or control in any way the Client’s transactions and have responsibility for the application of the practices, measures, procedures and controls that have been determined herein.

The AML Manual has been prepared to comply with:

- 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;
- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73);
- Sanctions National Ordinance (N.G. 2014, no. 55);

- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30);
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

These laws and regulations and any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law form the main legal basis for the Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons.

2.1 Purpose

The purpose of the AML Manual is to document the Company's internal practice, measures, procedures and controls relevant to the prevention of money laundering and terrorist financing and to further assist the Company's employees achieve the following objectives:

- Maintain the integrity, credibility and reputation of the Company;
- Implement and comply with all legal, regulatory requirements and reporting obligations that govern the sound operation of the Company;
- Provide and implement the processes for establishing a business relationship, the execution of occasional transaction(s) and the on-going monitoring of said business relationships and transactions;
- Enable the tracking, identification and evaluation of suspicious transactions/activities and protect the Company from possible fraud and other risks that may impact its economical status and reputation;
- Report any suspicious transactions for money laundering internally to the MLCO and externally to the Financial Crime Investigation Service;
- Be able to contribute to the investigation that might take place regarding a Client who may be under investigation for money laundering or terrorist financing activities, and to submit data on specific incidents relevant to those suspicious activities;
- Enable the development of a sound professional relationship with the Client.

2.2 Definition of Money Laundering

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering. It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement.* During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;

- b) *Layering*. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- c) *Integration*. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

2.3 Definition of Terrorism Financing

Financing of Terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.

The most basic difference between financing of terrorism and money laundering involves the origin of the funds. Terrorist financing uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While money laundering (ML) is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

2.4 Definition of Financing of Proliferation of weapons

Financing of proliferation (FP) is the provision of funds for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

2.5 Applicability

The provisions of the AML Manual are applicable to and expected to be implemented for all Clients, whether existing or prospective, in particular:

- a) When establishing a business relationship;
- b) When carrying out occasional transactions, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
- c) When there is suspicion for money laundering or terrorist financing activities, regardless of the amount of the transaction or other factors;
- d) When there are doubts about the veracity or adequacy of previously obtained Client identification data;
- e) When assessing the established Client business relationship, as part of the ongoing monitoring process and Client due diligence;

2.6 Supervisory Authorities

In accordance to the AML Law, the responsible supervisory bodies for approving instructions, guidance and regulations aimed at preventing money laundering and/or terrorist financing which are intended for casinos and providers of other online games shall be the Curacao Gaming Control Board (GCB).

2.7 Obligation perform Due Diligence measures as part of the Client Acceptance Process

The obligation of the Client identification and Client due diligence arises from the provisions of the AML Law. The aim of 'Know Your Client' (KYC) procedures is to understand and evaluate the level of risk entailed in prospective Clients' activities and to enable the Company to understand the Due Diligence measures necessary to be taken for ensuring a lawful Client acceptance. "KYC" is essentially achieved through the following due diligence procedures:

- proper identification of Clients;
- verification of the above specified information for the identity of the Client;
- the construction of the Client Economic Profile (hereinafter the “CEP”);
- the development and operation of efficient ongoing monitoring mechanisms in order to promptly identify any changes in Client’s economic profile and other important information;
- assessment of the overall profile and risk level of the Client resulting in the appropriate risk classifications (low, normal, high).

3. CLIENT ACCEPTANCE POLICY (CAP)

The Client Acceptance Policy (**Annex I**), following the principles and guidelines described in this AML Manual, defines the criteria for accepting and further classifying new Clients which shall be followed by the Company’s employees involved in the Client on-boarding process.

Generally, prior to the establishment of a business relationship the following procedures must be performed:

- a. Any potential client of the Company must complete a registration form and provide the necessary documentation.
- b. Identify the Client and verify the Client’s identity on the basis of data, documents or information obtained from reliable and independent sources.
- c. In case the Client - legal entity identify the beneficial owner and take adequate measures to verify his identity based on records, documents or information obtained from independent and reliable sources.
- d. Determine the Clients’ Risk Profile. Clients should be designated as high, low or normal risk.

The Client Acceptance Policy shall clarify the categories of prospective Clients with whom the Firm shall not proceed with the establishment of any business relationship or execution of any occasional transaction. The said policy should be revised on an annual basis. Furthermore, it shall specify the circumstances/situations where a business relationship with a Client may be terminated.

4. RESPONSIBILITIES OF THE BOARD OF DIRECTORS

It is a requirement that all employees of the Company involved in the KYC process, as well as the Directors of the Company understand and adhere to this Anti-Money Laundering Operations & Procedures Manual.

As the most senior management body of the Company, the Board of Directors (BoD) has a critical oversight role. The BoD approves and oversees policies relating to risk management and compliance. The Board also should have a clear understanding of the ML/TF risks, including timely, complete, and accurate information related to the risk assessment to make informed decisions.

The BoD is responsible appointing a qualified MLCO with overall responsibility for the AML/CTF function and provide the MLCO with sufficient authority that when issues are raised they get the appropriate attention from the BoD, the Director(s) and the business lines. The BoD is responsible for the overall AML/CTF compliance policy of the Company and ensuring adequate resources are provided for the proper training of staff and the implementation of risk systems.

The detailed responsibilities of the Board in relation to the prevention of money laundering and terrorist financing include the following:

- a) to determine, record and approve the general policy principles of the Company in relation to the prevention of money laundering and terrorist financing activities and to communicate those to the MLCO;
- b) to appoint the MLCO and, where is necessary, alternate MLCO, assistant MLCOs and determine their duties and responsibilities, which are recorded in this AML Manual;
- c) To ensure the designing and implementation of risk assessment practices and of an effective compliance management by monitoring and where needed enhancing the measures adopted;
- d) To ensure the recruitment of employees with impeccable integrity;

- e) to approve the AML Manual and to communicate it to all employees of the Company that manage, monitor or control in any way the Clients' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined;
- f) to ensure that all requirements of the AML Law and of the AML Order are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for effectively achieving the above mentioned requirement;
- g) to assure that the MLCO, the alternate MLCO and his assistants, if any, and any other person who has been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing (i.e. personnel of the Execution Department), have complete and timely access to all data and information concerning Clients' identity, transactions' documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties, as included herein;
- h) to ensure that all employees are aware of the person who has been assigned the duties of the MLCO, alternate MLCO, as well as the MLCOs assistants, if any, to whom they report, any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing;
- i) to establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the MLCO, either directly or through his assistants, if any, and notifies accordingly the MLCO for its explicit prescription in the Manual;
- j) to ensure that the MLCO and the alternate MLCO (if applicable) have sufficient resources, including competent staff and technological equipment, for the effective discharge of their duties;
- k) to assess and approve the MLCO's Annual Report in, and take all actions in a specific timeframe as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified in the abovementioned report;
- l) to meet and decide the necessary measures that need to be taken in a specific timeframe to ensure the rectification of any weaknesses and/or deficiencies which have been detected in the MLCO annual report.

5. MONEY LAUNDERING COMPLIANCE OFFICER (MLCO)

In accordance to Article V.3 of the AML Law, the Company shall formally designate a senior officer at management level and independent from the games operations, responsible for the detection and deterrence of money laundering and terrorist financing. The AML/CFT compliance officer must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The compliance officer must be able to act independently.

The compliance officer shall be assigned at least the following responsibilities:

- To design and implement the AML program;
- To verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing;
- To review compliance with the casino's policy and procedures;
- To organize training sessions for the staff on various compliance-related issues;
- To analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- To review all internally reported unusual transactions for their completeness and accuracy with other sources;
- To keep records of internally and externally reported unusual transactions;
- To execute closer investigation of unusual transactions if necessary;
- To prepare the external report of unusual transactions;
- To make necessary changes to the AML program;
- To remain informed on the local and international developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- To prepare periodic information on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

The MLCO is responsible for Transaction monitoring, receiving internal disclosures and making reports to the Curaçao Gaming Control Board (GCB). Additionally, the MLCO shall act as the first point of contact for all compliance issues from staff.

The MLCO undertakes regular random analysis of transactions including assessment of documentary evidence provided by Clients and prepares any necessary amendments to the Policy in line with the risk assessment. The MLCO ensures everyone is periodically informed of any changes in anti-money laundering and anti-terrorist financing legislation, policies and procedures, as well as current developments and changes in money laundering or terrorist activity financing schemes particular to their jobs, constructing AML/CTF-related content for staff training programs. Independently from front office staff, MLCO reviews Client identification information to ensure that all the necessary information has been obtained.

The employees should report to the MLCO about any information or other matter coming to their attention, and which in their opinion proves or creates suspicion that another person is engaged in a money laundering offence and/or terrorist financing. The information is received in a written report form (hereinafter the “Internal Suspicion Report”, a specimen of such report is attached in **Annex III**). The MLCO may discuss the circumstances of the case with the informer and where appropriate, with the informer’s superiors. The evaluation of the information shall be done on a report (hereinafter the “Internal Evaluation Report”, a specimen of such report is attached in **Annex IV**)

6. RISK BASED APPROACH

6.1 General

The Company’s Risk Based Approach is designed to target resources and efforts where the risk is greatest and, conversely, reduce requirements where the risk for ML & FT is low. The MLCO shall establish adequate and appropriate procedures relating to risk assessment and management in order to prevent operations related to money laundering or terrorist financing. These shall include:

- Determining the extent of customer due diligence measures on a risk-sensitive basis depending on the type of Client, business relationship, or services to be provided;
- The ability to demonstrate to supervisory authorities that the extent of customer due diligence measures is appropriate in view of the risks of money laundering and terrorist financing.
- Taking adequate measures to verify the identity of beneficial owners so that they are satisfied that they know who the beneficial owner is and what the control structure is in respect of a Client who is other than a natural person.
- Scrutinizing Clients’ transactions throughout the course of the business relationship to ensure consistency with businesses’ and individuals’ knowledge of the Client, the Client’s business and risk profile.
- Keeping up-to-date the information collected in applying customer due diligence measures.

The continuing threat of money laundering and terrorist financing is most effectively managed by understanding and addressing the potential money laundering and terrorist financing risks associated with Clients and transactions.

6.2 Risk factors specific to the Gambling Sector

The company uses a three-factor risk assessment (high, medium and low) in its work.

There are four risk areas:

1. Customer risk
2. Product, service and transaction risk
3. Geographical risk
4. Distribution channels risk

6.2.1 Customer risk

Determining the potential money laundering risks posed by a Client will provide significant input into the overall money laundering risk assessment. The MLCO will assess, whether a particular Client poses a higher risk of money

laundering and whether mitigating factors may lead to a determination that Clients engaged in such activities do not pose a higher risk of money laundering. Application of the risk variables described further below plays an important part in this determination. There is no universal consensus as to which Clients pose **a higher risk**, but the below listed characteristics of Clients have been identified with potentially higher money laundering risks:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

The following factors should also be considered in association with the Clients' characteristics and behaviour:

- Client transactions where there is no apparent legal financial/commercial rationale;
- Situations where the origin of wealth and/or source of funds cannot be easily verified;
- Unwillingness of Clients to provide information on the beneficial owners of a legal person;
- Transactions that are unnecessarily complex for their stated purpose;
- Transfers being made on behalf of a third party;
- Transactions that are inconsistent with financial standing or occupation, or are outside the normal course of business for the Client in light of the information provided by the Client when conducting the transactions or during subsequent contact (such as an interview) with the Client(s);
- Cases where the type and behaviour of Client falls outside the "norm", i.e. the common characteristics and behaviour patterns of the majority of the Company's Clients;
- Clients willing to pay unusual fees to have transactions conducted.

6.2.2 Product, service and transaction risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by casinos of specific payment methods, which are considered to present **a higher risk of ML/FT**, should also be treated as high risk factors. These include:

- Proceeds of crime. Risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- Cash. Land-based casinos (or physical establishments of online casinos) are used to exchange large amounts of illicit proceeds in small denominations for larger ones;
- Anonymous payment methods such as pre-paid cards and virtual assets;
- Use of casino accounts. This should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- Types of specific games (e.g. roulette, craps → even bets);
- Peer to peer gaming;
- The use by customer of accounts held or cards issued in the name of third parties;
- The transfer of funds from one gaming account to another;
- Types of financial services (credit/marker, currency exchange, check cashing);

- Multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- Changes to financial institution accounts to fund casino account;
- Identity fraud. Details of financial institution accounts stolen and used on web sites. Also stolen identities used to successfully open financial institutions accounts, and such accounts used on web sites;
- Using cash to fund a pre-paid card poses similar risks as cash;
- Games involving multiple operators (Poker on platforms shared by multiple operators);
- Electronic wallets (e- wallets). Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.

6.2.3. Distribution channels risk

The channels through which a casino establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction:

- Channels that favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;
- While situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the casino adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
- Where there is the involvement of a third party in the interactions between the customer and the casino, there is also an increase of risk. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations.

6.2.4. Geographical risk

The geographical risk is the risk posed to the casino by the geographical location of the player and the source of wealth of the business relationship. The nationality, residence and place of birth of the player have to be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction and countries which are known to have terrorist organizations operating are to be considered **as high risk**. It is advisable to take into account a variety of sources of information produced by the FATF and non-governmental well-known bodies. Some sources to use are:

- 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 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 sanctioned by the OFAC;
- Countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- Countries on the Corruption Perception Index compiled by Transparency International.

6.3 Technological developments risk assessment

The Company's should maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of money laundering or the financing of terrorism. It should identify and assess the money laundering or terrorist financing risks that may arise whenever:

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

In those cases, a risk assessment should take place prior to the launch of the new products, business practices, delivery mechanism or the use of new or developing technologies. This is done to determine whether the innovation creates a weakness that can be misused by money launderers or those seeking to finance terrorism. Such risk assessments must be documented. Where risks are identified, measures must be taken to mitigate these risks.

7. BUSINESS RISK ASSESSMENT (BRA)

Business Risk Assessment is established so as to monitor compliance with the policies introduced by the Company for the prevention and detection of ML/TF.

The MLCO is responsible to confirm adherence to various Anti-Money Laundering procedures through specifically designed reviews and/or other functional audits.

7.1 Assessment of the Business Risk Assessment

In order to effectively manage the risk of money laundering and terrorist financing, the MLCO must, at least once a year, perform an assessment (Business Risk Assessment) of the risk of money laundering and terrorist financing of its entire activity.

This risk assessment must be formalized in writing and submitted to the Board of Directors for further consideration. The report of the Business Risk Assessment should be covered, including:

- The methodology adapted;
- The reasons for considering a risk factor as presenting a low, medium or high risk;
- The outcome of the BRA;
- Any information sources used.

7.2 Money transfers to third parties

Generally, money transfers to third parties **are prohibited**. Transfers may only be made to/from accounts of the same Client.

Despite this, it is recognised that there may be certain cases where this may be required by law. For example, in the case of death, any money/assets in a Client's account should be able to be transferred to an heir. In such cases a full account review is triggered and the Accounting and Finance Department is not allowed to execute any third party transfers unless the following three conditions are all fulfilled:

- a. there is a written request for a transfer between accounts signed by both the transferor and the transferee;
- b. the transaction is approved by the Executive Director(s) after considering and examining all relevant information and circumstances.
- c. the transaction is approved by the MLCO after considering and examining all relevant information and circumstances.

7.3 Internal Investigations

Any suspicious transaction/activity, must immediately be reported to the MLCO. This report should be made in writing and before executing the Client's instructions to effect a suspicious transaction.

Suspicious monetary operations or an unusual transaction shall be also identified in accordance with the criteria for the identification of an unusual transactions or transactions according by the List of “INDICATIONS OF AN UNUSUAL TRANSACTIONS” (Annex II).

7.4 Escalation and reporting to the Financial Intelligence Unit Curaçao (FIU)

Company has to register with the FIU and to get access to the goAML reporting portal after validation by the FIU.

The compliance officer must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The casino shall report to the FIU the details of the transactions by means of the goAML reporting portal. The reports and the submission of the thereto related information (all supporting documents) should be done in English.

The casino and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

7.5. Tipping-off

Following a disclosure to FIU or any other supervisory institution, it is a criminal offence for anyone working in the Company, to do or say anything that might “tip off” Clients that such a disclosure has been made. If a SAR/STR has been filed, careful steps must be taken while communicating with Clients and additional advice should be taken from the MLCO who keeps a track of all internal investigations and escalations in order to not accidentally disclose investigative actions to Clients. No member of staff or personnel may disclose to the Client concerned or to a third party, the fact that an investigation is being carried out, or that information has been transmitted to the FIU, since such disclosure might prejudice any investigation being carried out. In the event that the Client is inadvertently alerted to ongoing investigations, the Company is to immediately seek guidance from the FIU as to how the Company should act.

7.6 Updating the Internal Control Procedures

In accordance to Low the Company must review and, if necessary, update its internal control procedures in the following cases:

- (a) upon the occurrence of important events or changes in the management and operation of the Company;
- (b) periodically monitoring the implementation and adequacy of internal control procedures;

8. CLIENT DUE DILIGENCE

8.1 Scope of Application

According of the AML Law establishes the requirement for the Company to take measures and identify its Clients' and the beneficial owners of its Clients as well as verify their identity prior to establishing a business relationship.

Additionally of the AML Law require that such measures are also required when there are doubts about the veracity or authenticity of the previously obtained identification data of the Client and of the beneficial owner or when there are suspicions that an act of money laundering and/or terrorist financing is, was or will be carried out.

Every reasonable effort should be made to determine the true identity of any person who asks to open an account, enters into a business relationship with the Company, or undertakes a significant one-off transaction or a series of linked transactions.

The Company shall not open any Client accounts and/or establish a business relationship and/or execute any one-off or several linked monetary operations before the Client due diligence is finalized.

8.2 Know your Client Principle (KYC)

“Know Your Client” processes are intended to enable a company to form a reasonable belief that it knows the true identity of each customer before the Client enters into a business relationship with the Company.

The need of effective KYC is at the very heart of an efficient anti-money laundering management system. KYC due diligence is a continuous process and not only limited to Clients seeking to open new accounts. While Client identification procedures are aimed at establishing Clients' identity, the Company is also required to decide whether the Clients' risk-profile necessitates enhanced due diligence procedures.

8.3 Due Diligence Procedures

According to the AML Law establishes the due diligence procedures that should be applied prior to establishing a business relationship with a Client. These procedures consist of:

- (i) taking measures to identify the Client and the beneficial owner as well as taking appropriate action to verify their identity;
- (ii) take all appropriate, targeted and proportionate measures to establish whether the Client acts on his own behalf or is controlled and to identify the beneficial owner and, where the Client acts through a representative, also identify that person;
- (iii) request and obtain documents and other data on the basis of which the Company would understand the ownership and management structure as well as the nature of activities of the Client which is a legal person;
- (iv) obtain from the Client information about the purpose and intended nature of the Client's business relationships;
- (v) verifying the identity of the Client and of the beneficial owner on the basis of the documents, data or information obtained from a reliable and independent source. In cases where a natural person who holds the position of senior managing official has been identified as a beneficial owner the Company must verify the identity of such natural person and must keep records of the actions taken as well as any difficulties encountered during the verification process;
- (vi) carrying out the ongoing monitoring of the Client's business relationships, including scrutiny of transactions undertaken throughout the course of such relationships, to ensure that the transactions being conducted are consistent with the Company's knowledge of the Client, its business and risk profile as well as the source of funds;
- (vii) regularly reviewing and keeping up-to-date documents, data or information submitted by the Client and the beneficial owner during due diligence process with a view to ensuring that they are appropriate and relevant;
- (viii) applying the Client and beneficial owner due diligence measures also to existing Clients, having regard to the level of risk, in the event of new circumstances or new information related to the determination of the level of risk posed by the Client and by the beneficial owner, their identification information, activities and other relevant circumstance;

Where during Client due diligence the Company has suspicions that an act of money laundering and/or terrorist financing is carried out and further Client due diligence may raise suspicions of the Client that information about him may be forwarded to the competent law enforcement institutions, the Company may discontinue the process of Client due diligence and not establish a business relationship with the Client.

8.4 Reliance on Third Parties for Client Identification

The Company may rely on third parties to apply any or all of the CDD procedures relating to verification of identity of the Client or beneficial owner and the nature and purpose of the intended business relationship, provided that such a third party is a respected and regulated professional/entity.

Company has also to regularly monitor and check whether its AML/CFT policies and procedures are properly implemented by the physical establishment. All the measures taken to guarantee compliance with the casino's measures must be documented.

9. SIMPLIFIED DUE DILIGENCE

9.1 Scope of Application

Simplified Client due diligence may be carried out where lower risk of money laundering and/or terrorist financing is identified based on the risk assessment and management procedures established by the Company in the cases of:

- (a) Not collecting specific information. If the risk assessment undertaken indicates a low risk of money laundering or terrorist financing then it is only necessary for the casino to obtain the player's identity. In this case casinos may limit identification to the first three personal details in paragraph III.2.1. in Low (full name, permanent residential address, date of birth)
- (b) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship
- (c) The extent of verification may also vary depending on the risk posed by the particular business relationship. In a low risk situation, the casino can also use alternative reputable information sources, even where these do not contain photographic evidence of the player's identity (e.g. birth certificates, bank statements etc.);
- (d) The extent of personal details verified can also vary. In low risk situations, the casino has to verify the basic identification details, while the verification of any other personal details is upon the casino, as long as it has sufficient comfort that it knows who its customer is;
- (e) Reducing the frequency of customer identification updates;
- (f) Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

Simplified CDD measures are not acceptable whenever there is suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply.

Where, in the course of performing ongoing monitoring of the Client's business relationships, it is established that the risk of money laundering and/or terrorist financing is no longer low, the Company must take the measures specified in Section 8.3 "Client Due Diligence" and identify both the Client and the beneficial owner as well as verify their identity.

10. ENHANCED DUE DILIGENCE

10.1 Scope of Application

Enhanced Client due diligence shall be carried out by applying additional measures of identification of the Client and of the beneficial owner **in addition** to those described in Section 8.

Enhanced Client due diligence shall be applied:

- a. Political Exposed Persons (PEP's)
- b. Residents of higher risk geographic areas
- c. Products or transactions that might favor anonymity
- d. 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;

The applied measures must be consistent with the risks identified. In particular, Company should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples of enhanced due diligence measures include:

- Obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;
- Obtaining additional information on the intended nature of the business relationship;
- Obtaining information on the source of funds or source of wealth of the player. Examples of source of funds include personal savings, employment, pension releases, share sales and dividends, property sales, gambling winnings, inheritances and gifts and compensation from legal rulings;
- Obtaining information on the reasons for intended or performed transactions;
- Obtaining the approval of senior management to commence or continue the business relationship;
- Conducting enhanced monitoring of the business relationship;

- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

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

10.2 Enhanced Due Diligence Procedures

(a) Politically Exposed Persons

When carrying out enhanced Client due diligence, where transactions or business relationships are carried out with politically exposed persons, the Company shall:

- 1) obtain approval from a senior manager for establishing business relationships with such Clients or continuing the business relationships with the Clients when they become politically exposed persons;
- 2) take adequate measures to establish the source of property and source of funds that are involved in the business relationship or transaction;
- 3) perform enhanced ongoing monitoring of the business relationships with politically exposed persons.

Although stricter customer due diligence is required for each PEP, this customer due diligence does not be the same for every PEP. The measures are tailored to the risk of the PEP, where the following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

This means that the measures taken can be tailored to the risks in a specific case.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, the casino must regularly screen for PEP status during the business relationship. Should a player who had not been identified as a PEP at onboarding stage result to have become one, the casino is required to implement the measures within the thirty-day window. Failing with these, will result in the casino to terminate the relationship with this customer.

(b) Residents of higher risk geographic areas:

- 1) countries identified, on the basis of data of reports or similar documents by the Financial Action Task Force on Money Laundering and Terrorist Financing or a similar regional organisation, as having significant non-conformities with international requirements in their anti-money laundering and/or combating the financing of terrorism systems;
- 2) countries identified, on the basis of data by governmental and universally-recognised non- governmental organisations monitoring and assessing the level of corruption, as having significant levels of corruption or other criminal activity;
- 3) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
- 4) countries provide funding or support for terrorist activities, or have designated terrorist organisations operating within their country.

(c) Products or transactions that might favor anonymity:

- 1) product or transaction might favour anonymity;
- 2) payments are received from unknown or unassociated third parties;

(d) 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

1) products and business practices, including delivery mechanism, are new and new or developing technologies are used for both new and pre-existing products

In the cases where higher risk of money laundering and/or terrorist financing is identified based on the risk assessment and management procedures laid down by the Company, the Company shall:

- 1) at its own discretion, apply one or several additional measures of identification of the Client and of the beneficial owner to decrease the risks posed;
- 2) obtain approval from a senior manager for establishing business relationships with such Clients or continuing business relationships with these Clients;
- 3) take adequate measures to establish the source of property and source of funds that are involved in the business relationships or transaction;
- 4) perform enhanced ongoing monitoring of the business relationships with such Clients.

10.3 The termination of the business relationship

If the client's due diligence obligations cannot be met, the Company will not enter into a business relationship or carry out any transactions and will terminate the business relationship with the client. The Company will also keep a record of all attempts made to obtain the necessary information and documentation. For this purpose, the Casino may decide either to close the account or to block it completely and suspend its operations.

If the customer provides the requested information and/or documentation to the company after the closure or suspension and blocking of the gaming account, the company should consider whether the delay in providing the requested documentation and/or CDD information affects the ML/FT risk associated with the gaming account, taking into account the business relationship.

The company should consider whether there are grounds for suspicion of ML/FT/AF. A customer's reluctance to provide CDD should not automatically equate to suspicion of ML/FT/AF. The firm should consider all the factors and information available to it in deciding whether there are grounds for suspecting ML/FT/AF. However, if there is a suspicion of ML/FT/AF, the casino must submit a report to the FIU regarding unusual transactions involving that player.

If there is no reason to withhold funds, they must be returned to the player. This should be done through the same channels used to receive the funds.

11. ONGOING MONITORING

11.1 General

After the proper due diligence procedure is undertaken and based on the results of the latter the Client is accepted, the further monitoring of the Client, the business relationship and monetary operations and transactions must be performed.

11.2 Ongoing monitoring

Ongoing monitoring is carried out to ensure that Clients meet the requirements stipulated in these AML Manual and that the Company's services are not used for any ML/TF purposes. The ongoing monitoring of a business relationship includes:

- the scrutiny of transactions to ensure that these are consistent with the Company's knowledge of the Client, his business and risk profile; and
- the scrutiny of transactions the amount of which is considered extraordinary compared to the size of regular transactions; and
- the monitoring of unusual patterns of transactions and/or complex or large transactions which have no apparent or visible economic or lawful purpose; and
- the monitoring of business relationships and transactions with persons from high risk jurisdictions; and

- ongoing monitoring of identity (If a change in identification information is detected, change of payment instrument);

The Company determines whether the changes are material, taking into account the risk of the customer, and reassesses the customer risk of the relationship if necessary.

11.3 Ongoing Transaction monitoring

Transaction monitoring is executed to prevent involvement of the casino with ML/TF and to safeguard the reputation of the casino. While in conducting ongoing scrutiny of transactions the Company notices that a customer's transactions are not consistent with what it knows or expects from the customer, the Company has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction. Source of funds refers to how the funds for a particular transaction were obtained by the player. The reason for inconsistency may lie in inconsistency, amongst others, with the source of funds or average profile or account activity noted to date).

The Company has to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction. It is also one of the situations in which the risk profile of the customer may have to be revised.

After receiving this information, the Company has to decide whether the transaction is an unusual transaction and need to be reported to the FIU.

As with anything else, the level of on-going monitoring will depend on the risk profile of the customer, but even in low risk situations there must be a degree of oversight taking place to ensure that the business relationship still has to be considered as a low risk one.

11.4 Ongoing monitoring of key risk factors

Ongoing monitoring of key risk factors shall consist of monitoring on a continuous basis if there are any changes in the following risk variables of a Client:

- (a) Politically Exposed Person;
- (b) Sanctioned Person;
- (c) Involved in criminal activity;

The above risk variables should not only be assessed during the initial on-boarding stage, but they should also be monitored on an ongoing basis after a business relationship is established with a Client in order to identify any possible changes and take appropriate action.

For the above purpose, the Company shall use the services of the specialized third party risk management **Sum and Substance Ltd** to conduct the above mentioned ongoing monitoring.

Sum and Substance Ltd is registered with the Information Commissioner's Office in line with the Data Protection Act 2018. Additionally, Sum and Substance Ltd has obtained the following certifications and attestations:

SOC 2 Type 1	SOC 2 Type 1 examination, which was proctored by independent auditor BARR Advisory, P.A. This assessment confirms that Sumsb has rigorous security controls against unauthorized access, disclosure or damage of data.
ISO/IEC 27001	This standard covers the security of development, implementation, functioning, monitoring, analysis, support and improvement of Sumsb's ISMS (Information Security Management System), which is audited on an annual basis.
ISO/IEC 27017	This certification demonstrates that Sumsb adheres to technical and organizational measures regarding risk assessments, equipment, software controls, personnel work, the backup procedure and other processes related to cloud service security.
ISO/IEC 27018	This certificate confirms that Sumsb has commonly accepted control objectives and guidelines for implementing measures to protect Personally Identifiable Information (PII) privacy principles in the public cloud computing environment.

PCI/DSS	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from major card schemes. This certification confirms that Sumsb is fully compliant with high standards for secure storage and processing of bank card data.
---------	---

11.5 Timing of CDD Measures

The casino conducts a comprehensive Customer Due Diligence measure when:

- a. When players engage in financial transactions equal to or above Naf. 4,0001 ;
- b. carrying out occasional transactions above the monetary equivalent of Naf. 4,000;
- c. there is a suspicion of money laundering or terrorist financing; or d. the casino has doubts about the veracity or adequacy of previously obtained customer identification data.

Note: a transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount in excess of the monetary equivalent of Naf. 4,000.

The threshold is calculated daily, taking into account all deposits and withdrawals made by the player since the establishment of a business relationship, including any peer-to-peer transfers. Once the threshold is reached, the Company conducts a PEP status check and risk assessment for customers, as well as fulfill its remaining CDD obligations.

When implementing the CD measures, customers are allowed to continue using their gaming account until the Company receives any necessary information from the relevant customer. However, if the threshold of 4,000 francs is reached, the player will not be able to deposit funds into the account or withdraw them from the account. In addition, if the requested information and documentation are not received within 30 days of reaching the threshold of 4,000 Swiss francs required to complete the CDD, the Company will terminate the relationship with the player and report the transaction to the FIU.

11.6 Reliance on third parties to perform customer due diligence

In its activities, the Company does not involve third parties in the performance of elements a-c of the CDD measures.

12.TERMINATION OF BUSINESS RELATIONSHIP AND PROHIBITION OF DISCLOSURE

Where the Client avoids or refuses to submit additional information to the Company, at its request and within the specified time limits, the Company may, refuse to execute monetary operations or transactions and terminate the business relationship with the Client.

The Company shall maintain a register (in the form of **Annex VI**) of the Clients with whom transactions or business relationships were terminated under the circumstances specified above or under any other circumstances related to violations of the procedure for the prevention of money laundering and/or terrorist financing.

The above register data shall be stored in paper or electronic form for eight years from the date of termination of transactions or business relationships with the Client.

The Company may terminate business relationship / decline to start it or cancel Client's transaction when:

- Upon request and within provided timelines Client did not provide or refused to provide information or documents requested;
- Client is not able to prove his Source of Wealth or Funds when this is requested, or provided information and documents suggest that Client gained income from questionable or higher risk activity (precious metals, dual use goods, guns proliferation, etc.);

- Client gave false information about themselves and/or their activities or intentionally concealed certain information;
- Client has or had connections/links with organized criminal organizations (according to reliable information from competent national authorities or provided by international organizations/institutions);
- Fraudulent acting of the Client was proved in relation to the use of the Company services;

The MLCO is responsible to investigate each case before deciding to terminate/ decline to start a business relationship or cancel a Client's transaction.

Every employee must follow the "tipping off" rule – if an employee, especially communicating directly with a Client, knows that the Client's account is being terminated as a result of reporting him /her to FIU, such information cannot be shared directly or indirectly with the Client under any circumstances.

13. RECORD KEEPING

The Company must keep the following records:

(1) Client Due Diligence:

- a. all records of steps taken to obtain identification records, as well as copies of evidence of the identity of the Clients and beneficial owners as the case may be.
- b. all risk assessment records as well as the Client risk profile;
- c. all records relating to source of funds and source of wealth;
- d. all records related to the ongoing monitoring of the Clients;

(2) Record of Transactions:

- a. records containing details of all transactions undertaken in the course of an established Business relationship; this is to include a record of all work performed for or the services provided to the Clients;
- b. transaction records are to be kept in a form which will allow a satisfactory audit trail to be completed where necessary, and which may establish a financial profile of any suspect Client;
- c. records on internal and external Suspicious Monetary operations and Transactions reporting.

(3) Other Records:

- a. evidence of the training programmes on ML/TF prevention whether in-house or external;
- b. evidence of the proper acknowledgment of the Employees with these Procedures and their amendments as may be needed from time to time;
- c. other records if required under these Procedures or the Law.

The Company maintains the electronic Registers indicated below:

1.	Register of STR_SAR	To be maintained for 5 years after terminating business relationship;
2.	Register of sanctioned persons	
3.	Register of PEP Clients	
4.	Log of all Client transactions	
5.	Log of business relationships terminated due to ML/TF reasons	
6.	Copies of ID documents, identification information and KYC information	

7.	Correspondence with Client	To be maintained for 5 years after terminating business relationship
8.	Supporting documents obtained from Client	To be maintained for 8 years after completing transaction
9.	Internal investigation records of suspicious transactions	To be maintained for 5 years after terminating business relationship;
10.	Other records	To be maintained for 5 years after terminating business relationship;

The Registers are managed in digital format. The Registers are stored on the servers of the Company and are accessible via the internal network of the Company only. Records may be kept both in hard copies and in soft copies, save the Registers which are kept in digital format only.

14. TRAINING OF EMPLOYEES

All staff and kept personnel (New employees, Dealers, cashiers and slot department personnel, Audit staff, AML Compliance staff, Supervisors and Managers, Senior management and board of directors), whose duties include the handling of Clients' business, are to be adequately trained with respect to the procedures and the provisions of the Prevention of Money Laundering Act, the relevant Regulations and AML Manual.

The level of training provided to individuals is to be appropriate to their role and seniority within the Company. In any case all Employees must have the proper training on ML/TF prevention prior to the commencement of their duties at the Company which involve the ML/TF risk.

The MLCO prepares and implements, on an annual basis (or whenever deemed necessary), an educational training program (training plan) for staff depending on the needs of the Company regarding the prevention of using the financial system for money laundering or other illicit purpose, including preventive developments and practical methods and trends used.

The MLCO shall evaluate the adequacy of the seminars and the training provided to the staff and maintains detailed data regarding the seminars/ programs carried out, such as:

- Details on the content of the training programs
- The names of the staff members who have received the training
- The date on which the training was provided
- The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements

ANNEX I – CLIENT ACCEPTANCE POLICY

1. Introduction

The purpose of the Company's Client Acceptance Policy (hereinafter the "Policy") is to lay down the procedures and the control systems based on which the Company operates during the process of accepting new customers. The Client Acceptance Policy has been prepared so that it complies with requirements of the law for the prevention of money laundering and terrorist financing (AML Law).

The Company, during the on boarding process, should collect the documents which are sufficient to identify the Client, and in case of legal entities, the beneficiaries of the legal entity. The detailed requirements for the documents to be collected for various categories of Clients are described further in this AML Manual.

The MLCO shall be responsible for the implementation of the Client Acceptance Policy (CAP). In this respect, the MLCO shall be expected to seek and obtain satisfactory evidence of the identity of every Client before establishing a business relationship or before the execution of an occasional transaction.

The Company takes a risk-based approach in the implementation of measures and procedures so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be higher. The risk-based approach adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed.

2. General Principles of the Client Acceptance Policy

The General Principles of the CAP consist of:

- a) where the Client is a prospective Client, a Client account must be opened only after the relevant account opening due diligence, identification and verification measures and procedures have been conducted;
- b) all documents and data required as per the CAP must be collected before accepting a new Client;
- c) no account shall be opened in anonymous or fictitious names(s);
- d) no account shall be opened unless the prospective Client is approved by the MLCO;

3. Prohibited Clients and Transactions

Certain types of Client/transactions are not accepted for establishing business relationships or conducting transactions in order to reduce the risk that the services and products of the Company may be used for money laundering or terrorist financing or other illicit purposes and at the same time for protect the Company from the financial, reputational and legal risks.

Consequently, it is strictly prohibited to:

- a) Establish a business relationship with Clients who fail or refuse to submit the requisite data and information for the verification of their identity and the creation of their economic profile, without adequate justification.
- b) Establish a business relationship and/or conduct transactions with natural or legal persons against which sanctions prohibiting such relationship/transactions are imposed in accordance to the Company's Sanctions Policy (**Annex V**).
- c) Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons whose activities are related to criminal activity.
- d) Establish a business relationship or conduct transactions that involve in any way, directly or indirectly, natural or legal persons where:
 - Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients acting on behalf of Specially Designated Nationals and Blocked Persons (SDNs);
 - Clients whose source of funds (SoF) and source of Wealth (SoW) were generated from a sanctioned activity;
 - Clients whose source of funds (SoF) and source of Wealth (SoW) cannot be verified when this is required;
 - Transactions with third parties ultimately owned or controlled, directly or indirectly, by sanctioned parties;
- e) Establish a business relationship and/or conduct transactions with natural persons residing in a jurisdiction/country where it is prohibited by Company policy to offer its services to. Prohibited jurisdictions / countries are provided in the (**Annex VII**)

4. High Risk Clients

The below categories of Clients shall by default be classified as “High Risk” Clients irrespective of any other client specific risk variables:

- Customers who have multiple sources of income;
- Customers with irregular income streams;
- PEPs;
- High spenders (money can be derived from illegal activities);
- Disproportionate spenders (inconsistent with casino’s information about customer’s known source of income/assets);
- Casual customers like locals/tourists, especially when spending pattern changes;
- Improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- Multiple casino player rating accounts to hinder a casino to track their gambling activities;
- Unknown customers (redeeming large amounts of chips);
- Junkets (junket operators monitor player activity and issues and collect credit).

5. Client Approval Process

Before accepting a new Client, MLCO needs to study the Client and determine the final result of the review, i.e. approve or reject a potential Client.

The MLCO who is responsible for analyzing the information presented by the Client must seek further information from external or 3rd party sources, to enable or reinforce his opinion with respect to accepting a new Client or not. The decision to accept or reject a Client lies firstly with the MLCO and then with the Senior Management who give final approval for account opening.

If the MLCO rejects the Client, then the Client cannot be accepted.

6. Identification requirements and verification procedures of a physical person

This section refers to individuals who directly or indirectly establish a business relationship with the Company (e.g. direct Clients, beneficial owners, authorized persons, etc.). The Company should be satisfied that it is dealing with a real person and obtain sufficient evidence of identity to establish that a prospective Client is who he/she claims to be.

Documents for Client’s identification is provided in English language. In the case of execution of original documents in another language, the Client independently prepares the translation with its appropriate certification. The Client is responsible for the accuracy of the information contained in the submitted documents, including the quality of the translation.

Document verification is intended to prevent the following issues:

- Forgery
- Data tampering
- Photo replacement
- Fraud
- Using document printouts
- Other manipulation

The ID document must contain as minimum the following information:

- Owner full name
- Owner full date of birth
- Document number
- Validity data (issue date or validity period)
- Owner photo
- Owner signature (if applicable)

The ID document should meet the following requirements:

- The document is valid for at least one month from the upload date.
- The document is not scratched, stained, or torn.
- The applicant full name, date of birth and other important information is present and can be read.

(a) Non-face to face identification procedures

The process of ID document verification for non-face to face Clients consists of 4 steps:

(1) Uploading the photo of an ID document

The photo of the ID document uploaded to the system should meet the following requirements:

- The uploaded file is an original photo (static image) or scan (not a screenshot or a photo uploaded from social networks) in JPG, JPEG, PNG, PDF.
- If the document has data on the front and back, both sides should be uploaded.
- The size of the uploaded file is no less than 100 KB or 300 DPI.
- The photo is in color.
- The information in the document is readable.
- All corners of the document are visible and no foreign objects or graphic elements are present.
- The uploaded photo has not been edited with any software or converted to PDF.
- The document is not digital (in most cases).

(2) Checking the image for authenticity

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image receives a digital trust score:

- Low – red (high risk of editing).
- Acceptable – yellow (there might be something to take a closer look at).
- Normal – green (a trusted and authentic image).

(3) Checking image integrity

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents. Integrity checks consist of:

- General conformity to the template.
- Presence of security features, such as watermarks, holograms, and so on.
 - Font originality and compliance with the relevant standards (width, spaces between the letters, and so on.).
- Required fields and inscriptions.

(4) Document data validation

At the final step, the data extracted from the document is checked against various sources, including sanctions and watchlist databases.

7.Supported Identification Documents

The following Identification documents are supported.

Country	Document type	Country	Document type	Country	Document type
Argentina	Passport – biodata page only	Hong Kong	Passport – biodata page only	Netherlands	Passport – biodata page only
	Diplomatic Passport – biodata page only		ID Card – front side		Travel Document – biodata page only
	Provisional Passport (Pasaporte de Emergencia)		Mainland Travel Permit - back side required		ID Card – back side required
	ID Card – back side required		Consular Corps ID Card - front side		Bonaire ID – back side required
	Booklet ID – front side	Hungary	Passport – biodata page only		Diplomatic ID – back side required
	Diplomatic ID – back side required		Emergency Passport – biodata page only		Sint Eustatius ID – back side required
	Driving License:		ID Card – back side required		Saba ID– back side required
	Provincia de Entre Rios – front side		Booklet ID – front side		Driving License – back side required
	Ciudad Autonoma de Buenos Aires – back side required		Temporary – back side required		Residence Permit – back side required
	Santa Fe – back side required		Driving License – front side	Norway	Passport – biodata page only
	Provincia de Buenos Aires – back side required		Residence Permit – back side required		Travel Document – biodata page only
	Santiago del Estero – back side required		Kishatarforgalmi Engedely – front side		Seafarer's Identity Document – biodata page only
	Cordoba – back side required		Foreigner ID – front side		Immigrant Passport – biodata page only
	Provincia de Mendoza – front side	Iceland	Passport – biodata page only		ID Card – back side required
	Residence Permit – back side required		ID Card – front side		Army / Military ID Card – front side
Armenia	Passport – full spread		Driving License – front side		Driving License – back side required
	ID Card – back side required		Residence Permit – back side required		Residence Permit – back side required
	Driving License – back side required	India	Passport – biodata page only	Paraguay	Passport – full spread
	Residence Permit – back side required		Overseas Citizen of India Certificate of Registration – biodata page only		ID Card – back side required
Austria	Passport – full spread		ID Card (Aadhaar) – back side required		Driving License – back side required
	Emergency Passport – biodata page only		Digital ID – back side required	Peru	Passport – biodata page only
	ID Card – back side required		Ex Servicemen ID Card – back side required		ID card – back side required
	Diplomatic ID – back side required		Border Police Force ID – back side required		Children ID – back side required
	Disabled Person Card – front side		Indian Armed Forces Civilian Card – back side required		Military ID – back side required
	Driving License – back side required		Islanders Identity Card (Andaman and Nicobar) – back side required		Certificado de Inscripción – front side
	Residence Permit – back side required		Permanent Account Number Card – front side		Ministerio de Relaciones Exteriores – front side
Bahrain	Passport – biodata page only		Post Office ID Card – back side required		Carné de Solicitante de Refugio – back side required
	Diplomatic Passport – biodata page only		Resident Identity Card – front side		Driving License – back side required

	Special Passport – biodata page only		Tax ID – front side		Municipalidad de Huancayo – back side required
--	--------------------------------------	--	---------------------	--	--

Country	Document type	Country	Document type	Country	Document type
	ID Card – back side required		Voter ID – back side required		Municipalidad de Cajamarca – back side required
	Driving License – back side required		Ration Card – front side		Municipalidad de Callao – back side required
Belgium	Passport – biodata page only		e-SHRAM Card – back side required		Municipalidad de Ica – back side required
	ID Card – back side required		Driving License requirements:		Municipalidad de Canta – back side required
	Carte d'identité diplomatique (spéciale) – back side required		Andhra State DL – back side required		Municipalidad Mariscal Nieto – back side required
	Driving License – front side		Arunachal State DL – back side required		Municipalidad de Canete – back side required
	Provisional – front side		Assam State DL – back side required		Municipalidad de Caylloma – back side required
	Residence Permit – back side required		Bihar State DL – front side		Municipalidad de Melgar – back side required
	E Card (EU Citizen) – back side required		Chandigarh State DL – front side		Municipalidad de Maynas – back side required
	F Card (Member of EU Citizen Family) – back side required		Chhattisgarh State DL – back side required		Residence Permit – back side required
	E Plus Card (EU Citizen) – back side required		Delhi state DL – front side	Poland	Passport – biodata page only
Bolivia	Passport – biodata page only		Goa State DL – front side		Temporary Passport – biodata page only
	ID Card – back side required		Gujarat State DL – front side		Travel document – biodata page only
	Military ID – front side		Haryana State DL – back side required		ID Card – back side required
	Driving License – back side required		Hoshiarpur State DL – front side		Karta Polaka – back side required
	Residence Permit – back side required		Booklet DL – front side		Military ID – front side
Brazil	Passport – full spread		Indian Union DL – back side required		Special ID – back side required
	ID Card – back side required		Jalandhar State DL – front side		Driving License – back side required
	Civil Aviation Agency Card – front side		Jammu and Kashmir state DL – back side required		Residence Permit – back side required
	Carteira Especial De Identidade – back side required		Jharkhand state DL – front side		Zezwolenie mały ruch graniczny – back side required
	Army / Military ID Card – back side required		Karnataka state DL – back side required	Portugal	Passport – biodata page only
	Labor Card – back side required		Kerala state DL – back side required		ID Card – back side required
	Military Service Exemption Certificate – back side required		Madhya state DL – front side		Driving License – back side required
	Federal Council of Administration Card – back side required		Maharashtra state DL – back side required		Residence Permit – back side required
	Federal Council of Physical Education Card – back side required		Manipur state DL – back side required		EU citizen family member card – back side required
	Federal Nursing Council Card - back side required		Meghalaya state DL – back side required		Permanent Residence EU Citizen card – back side required
	Federal Council of Engineering and agronomy card – front side		Mizoram state DL – back side required	Puerto Rico	Passport – full spread
	Federal Council of Pharmacy Card – front side Federal Council of Medicine card -back side required		Nagaland state DL – back side required		ID Card – back side required
	Federal Council of Veterinary Medicine – back side required		Odisha (Orissa) state DL – front side		Voter ID – back side required

	Federal and Regional Council of Dentistry Card – back side required		Pondicherry (Puducherry) state DL – back side required		Firearms License – back side required
	Regional Council Economy Card – back side required		Punjab state DL – back side required		Driving License – back side required
	Regional Accounting Council Card – back side required		Rajasthan state DL – front side	Republic of South Africa	Passport – full spread
	Regional Council of Economics Card – back side required		Sikkim state DL – front side		ID Card – back side required
	Regional Council of Psychology Card – back side required		Tamil Nadu state DL – back side required		Booklet ID – front side

Country	Document type	Country	Document type	Country	Document type
	Council of Architecture and Urbanism of Brazil Card – back side required		Tripura state DL – back side required		Temporary ID – front side
	Consul ID - back side required Functional identity Card – back side required		Telangana state DL – back side required		Residence Permit requirements:
	Ministry of Defence Cards – back side required		Uttar state DL – back side required		Asylum Seeker Temporary Permit – front side
	Ministry of Justice Card – back side required		West Bengal state DL – back side required	Romania	Passport – biodata page only
	Bar Association of Brazil Card – back side required		Central Motor Vehicles – back side required		Temporary Passport – biodata page only
	Military Police Card – back side required		Union of India DL – back side required		ID Card – back side required
	Secretariat of Social Defense Card – back side required		Uttarakhand DL – back side required		Provisional ID – front side
	Secretary of State of Seguranca Publica Card – back side required	Indonesia	Passport – full spread		Driving License – back side required
	COFECI CRECI system Card – back side required		Service Passport – full spread		Residence Permit – back side required
	Driving License – back side required		Diplomatic Passport – full spread		Permis De Mic Trafic De Frontiera – back side required
	Circulação Internacional de Automotores – back side required		ID Card – front side	Saudi Arabia	Passport – full spread
	Carteira de Habilitação do Amador – front side		Surat Keterangan – front side		Diplomatic Passport – biodata page only
	Residence Permit – back side required		Driving License – front side		Special Passport – biodata page only
	Alien Identity Card – back side required		Residence Permit – back side required		ID Card – back side required
Bulgaria	Passport – biodata page only		Limited Stay Permit Card – front side		ID Card (please contact us) – front side
	Temporary Passport – biodata page only	Ireland	Passport – biodata page only		Driving License – back side required
	ID Card – back side required		ID Card – back side required		Residence Permit – front side
	Card of Subsidiary Protection Beneficiary – back side required		Military ID – front side		Saudi Premium Residence – front side
	Driving License – front side		Driving License – front side		Residence permit (please contact us) – front side
	Residence Permit – back side required		Residence Permit – back side required	Singapore	Passport – biodata page only
Chile	Passport – biodata page only	Isle of Man	Passport – biodata page only		ID Card – back side required
	Emergency Passport		Driving License – front side		Home Team National Service Identity Card – back side required
	ID Card – back side required	Italy	Passport – biodata page only		Driving License – back side required
	Residence Permit – back side required		Travel document – biodata page only		Residence Permit – back side required
Colombia	Passport – biodata page only		ID card – back side required		Employment Pass – back side required
	Temporary – biodata page only		Army / Military ID Card – back side required		Work Permit – back side required
	Foreign – biodata page only		Diplomatic ID – back side required		Student's Pass – back side required

	ID Card – back side required		Booklet ID – back side required		Dependant's Pass – back side required
	Consul ID – back side required		Driving License – back side required		EntrePass – back side required
	Permiso Especial de Permanencia - front side		Booklet DL – back side required	Slovakia	Passport - biodata page only
	Driving License – front side		Residence Permit – back side required		ID card - back side required
	Residence Permit – back side required		Booklet RP – front side		Driving License - front side
Costa Rica	Passport – biodata page only	Japan	Passport – biodata page only		Paper card - back side required
	ID Card – back side required		Re-entry Permit – biodata page only		Residence Permit - back side required
	Driving License – front side		ID Cards:	Slovenia	Passport – biodata page only
	Residence Permit – back side required		My Number Card – front side		ID Card – back side required
	Work permit – front side		Ground Self-Defense Force Personnel card – back side required		Driving License – front side

Country	Document type	Country	Document type	Country	Document type
Croatia	Passport – biodata page only		Residential Land and Building Trader Certificate – front side		Residence Permit – back side required
	ID Card – back side required		Driving License – back side required		Family Member Card – back side required
	Driving License – back side required		Provisional Driving License – back side required	Spain	Passport – biodata page only
	Residence Permit – back side required		Voluntary Returned Driving License – back side required		ID Card – back side required
Cyprus	Passport – full spread		Residence Permit – back side required		Diplomatic ID – back side required
	ID Card – back side required		Zairyi Card – back side required		Driving License – front side
	Driving License – front side		Basic Resident Registration Card – back side required		Guardia Civil License – front side
	Residence Permit – back side required	Jersey	Passport – biodata page only		Residence Permit – back side required
Czechia (Czech Republic)	Passport – biodata page only		ID Card – no National ID:		Asylum Seeker ID – front side
	Cestovni prukaz totoznosti – biodata page only		Citizenscard, Totum ID, Young Scot – front side	Sri Lanka	Passport – biodata page only
	ID Card – back side required		Driving License – front side		ID Card – back side required
	Diplomatic ID – back side required	Kazakhstan	Passport – biodata page only		Paper ID (translation required) – back side required
	Disabled person ID – back side required		Diplomatic Passport – biodata page only		Military ID – front side
	Driving License – front side		Alien Passport – biodata page only		Driving License – front side
	Residence Permit - back side required		Service Passport – biodata page only		Learners Permit – front side
Denmark	Passport – biodata page only		ID Card – back side required	Sweden	Passport – biodata page only
	Army / Military ID Card – front side		Driving License – front side		Emergency Passport – full spread
	Legitimationskort – front side		Residence Permit – back side required		Diplomatic Passport – biodata page only
	Driving License – front side	Kuwait	Passport – biodata page only		Aliens Passport – biodata page only
	Residence Permit – back side required		ID card – back side required		ID Card – back side required
Dominica	Passport – biodata page only		Stateless person card (please contact us) – back side required		Tax ID – front side
	Multi-purpose ID card – back side required		Driving License – back side required		Identitetskort – front side
	Driving License – front side	Kyrgyzstan	Passport – biodata page only		Driving License – back side required
Dominican Republic	Passport – biodata page only		ID card – back side required		Residence Permit – back side required

	ID Card – back side required		Passport Card – back side required	Switzerland	Passport – full spread
	Voter card – back side required		Driving License – front side		Temporary – full spread
	Consul ID – back side required	Latvia	Passport – full spread		ID Card – back side required
	Driving License – back side required		ID card – back side required		Diplomatic ID – back side required
	Residence Permit – front side		Latvijas Nepilsonis – back side required		Driving License – back side required
	RT-9 card – back side required		Driving License – back side required		Learner's Permit – front side
Ecuador	Passport – biodata page only		Learner's Permit – back side required		Residence Permit – back side required
	Diplomatic Passport – biodata page only		Residence Permit - back side required	Tanzania	Passport – biodata page only
	ID Card – back side required	Lebanon	Passport – full spread		ID Card – back side required
	Consul ID – back side required		ID Card (please contact us) – front side		Voter ID – front side
	Driving License – front side		Consul ID – front side		Zanzibari Card – back side required
	Residence Permit – back side required		Driving License – back side required		Health Insurance – front side
El Salvador	Passport – biodata page only		Laminated paper card (please contact us) – front side		Zanzibar Voter ID – front side
	ID Card – back side required		Residence Permit – back side required (some may require notarized translation)		Driving License – back side required
	Driving License – back side required	Lithuania	Passport – biodata page only		Zanzibar DL – front side
	Residence Permit – back side required		ID card – back side required		Residence Permit:

Country	Document type	Country	Document type	Country	Document type
Equatorial Guinea	Passport – biodata page only		Driving License – front side		E-Permit Card – back side required
	ID Card – back side required		Residence Permit – back side required	Thailand	Passport – biodata page only
	Driving License – back side required	Luxembourg	Passport – biodata page only		Border Passport – biodata page only
	Residence Permit – back side required		ID Card – back side required		Emergency Passport – biodata page only
Estonia	Passport – biodata page only		Driving License – front side		ID Card – front side
	Alien's Passport – biodata page only		Residence Permit – back side required		Army ID – front side
	ID Card – back side required	Madagascar	Passport – full spread		Card for not registered – front side
	Driving License – front side		Service Passport – full spread		Persons with Disabilities ID – front side
	Residence Permit – back side required		ID Card – back side required		Radio Operator License – front side
Finland	Passport – biodata page only		Driving License – back side required		Driving License – back side required
	Diplomatic Passport – biodata page only		DL in form of a booklet – front side		Temporary DL – back side required
	ID Card – back side required		Residence Permit – back side required		Public Vehicle DL – back side required
	Minor's ID – front side	Malaysia	Passport – full spread		Life Time DL – front side
	Driving License – front side		ID Card – front side		Residence Permit – front side
	Pahvinen Ajokortti (Cardboard License) – back side required		MyKAS Card – front side		Work Permit – back side required
	Residence Permit – back side required		Military ID – front side	Turkey	Passport – biodata page only
France	Passport – full spread		Driving License – front side		ID Card – back side required
	Emergency Passport – full spread		Learner's DL – front side, should be accompanied by expiry date slip		Diplomatic ID – back side required
	Diplomatic Passport – biodata page only		Vocational License – front side		Gecici Koruma Kimlik Belgesi – front side

	Service Passport – full spread		Residence Permit – front side		Uluslararası Koruma Basvuru Sahibi Kimlik Belgesi – front side
	ID card – back side required		Student Pass – back side required		Driving License – back side required
	Army / Military ID – back side required		Work Permit Service Card –back side required		Residence Permit – back side required
	Diplomatic ID – back side required		Sticker RP – front side		Work Permit – back side required
	Carte Individuelle d'Admission a l'Aide Médicale de l'Etat – front side	Malta	Passport – biodata page only		Blue Card – back side required
	Gendarmerie Nationale – back side required		ID Card – back side required	Ukraine	Passport – full spread
	Driving License – front side		Driving License – front side		Temporary Certificate of Citizenship – biodata page only
	Residence Permit – back side required		Residence Permit – back side required		Travel Document of Person Granted Complementary Protection – biodata page only
	DCEM Minor Permit - back side required	Mexico	Passport – biodata page only		Internal old passport (at request) – full spread
	Récépissé (Renewal Receipt) – front side		ID Cards:		Foreign – full spread
	Attestation de Demande d'Asile – front side		Military ID – back side required		Seafarer's – full spread
	Récépissé Constatant la Reconnaissance D'une Protection Internationale – front side		Consular ID – back side required		ID Card – back side required
	Autorisation Provisoire de Sejour – front side		Secretary of Public Education Card – back side required		Army ID – front side
Georgia	Passport – full spread		Voter ID – back side required		Pension Certificate – front side
	ID Card – back side required		Driving License requirements:		Driving License – front side
	Driving License – back side required		Aguascalientes state DL – back side required		Residence Permit – front side
	Residence Permit – back side required		Baja California state DL – back side required		Temporary Residence Permit – back side required
	Temporary Residence Permit Card – back side required		Baja California Sur state DL – back side required		Permanent Residence Permit – back side required
Country	Document type	Country	Document type	Country	Document type
Germany	Passport – biodata page only		Campeche state DL – back side required	United Kingdom	Passport – full spread
	Reisepass – full spread		Cancun DL – back side required		Travel Document – full spread
	Passersatz – full spread		Chiapas state DL – back side required		Emergency Passport – full spread
	Reisepass (Travel document) – biodata page only		Chihuahua state DL – front side		British Overseas Territories Passport – full spread
	ID Card – back side required		Chihuahua (Chofer Particular) – back side required		ID Card – no National ID:
	Temporary ID – back side required		Mexico city DL – back side required		Citizenship Card, Totum ID, Young Scot – front side
	Diplomatic ID – back side required		Coahuila State DL – back side required		Electoral ID – front side
	Driving License – front side		Colima state DL – back side required		Driving License – front side
	Residence Permit – back side required		Durango state DL – back side required		Provisional – front side
	Asylum ID – back side required		Federal DL – back side required		Welsh (Cymraeg) – front side
	Toleration Status Card – back side required		Guerrero state DL – back side required		Brexit design – front side
Gibraltar	Passport – biodata page only		Guanajuato state DL – back side required		Northern Ireland design – front side
	Emergency Passport – biodata page only		Estado de Mexico – back side required		Residence Permit – back side required

	ID Card – back side required		Hidalgo state DL – back side required	Vietnam	Passport – full spread
	Civilian Registration Card – back side required		Jalisco state DL – back side required		Entry and Exit Permit – biodata page only
	Driving License – front side		Mexico state DL – back side required		ID card – back side required
Greece	Passport – full spread		Michoacan state DL – back side required		Military ID – back side required
	Service Passport – biodata page only		Morelos state DL – back side required		Driving License – front side
	Diplomatic Passport – biodata page only		Nayarit state DL – back side required		Army DL – front side
	ID Card - back side required		Nuevo Leon state DL – back side required		Residence Permit – front side
	Army / Military ID Card – back side required		Oaxaca state DL – back side required		Temporary Resident Card – front side
	Air force ID – back side required		Puebla state DL – back side required		Permanent Resident Card – back side required
	Marine ID – back side required		Queretaro state DL – back side required		Certificate of Visa Exemption – front side
	Fire corps ID – back side required		Quintana Roo state DL – back side required		
	National defence ID – back side required		San Luis Potosi state DL – back side required		
	International Protection Applicant Card – back side required		Sinaloa state DL – back side required		
	Driving License – front side		Solidaridad state DL – back side required		
	Residence Permit – back side required		Sonora state DL – back side required		
Greenland	Passport – biodata page only		Tabasco state DL – back side required		
	Driving License – front side		Tamaulipas state DL – back side required		
Guatemala	Passport – biodata page only		Tlaxcala state DL – back side required		
	ID Card – back side required		Tulum city DL – back side required		
	Consular ID – back side required		Veracruz state DL – back side required		
	Driving License – back side required		Yucatan state DL – back side required		
Honduras	Passport – biodata page only		Residente Permanente Card – back side required		
	ID Card – back side required	Moldova	Passport – biodata page only		
	Consul ID – back side required		ID Card – back side required		
	Driving License – back side required		Driving License – back side required		

For other countries, not listed above, an international passport (biodata page only) or a valid national identity card may be considered. Other documentation may be considered on a case-by-case basis and following the approval of the MLCO.

8. Proof of address verification

(a) Non-face to face procedures

The process of Proof of Address (PoA) document verification for non-face to face Clients consists of the following steps:

- **Uploading a PoA photo.**

By default, the system accepts PoA documents that have been issued within the last 3 months.

- **Checking the image for authenticity.**

The image authenticity check is intended to ensure that the uploaded image has not been edited electronically. This process involves automated signature analysis.

A software signature includes file metadata, compression parameters, vendor or software-specific tags, sections, and so on. An extensive database of camera and software signatures are utilized to determine the source of an image, detect traces of modification software, and estimate the risk of intended image tampering (as opposed to cosmetic changes like cropping, resizing, or rotation).

Each image receives a digital trust score:

- Low – red (high risk of editing).
- Acceptable – yellow (there might be something to take a closer look at).
- Normal – green (a trusted and authentic image).

- **Checking the integrity of the image.**

Integrity checks are designed to ensure the uploaded image represents an official document by comparing it with a template from a database of original documents. Integrity checks consist of:

- General conformity to the template.
- Font originality and compliance with the relevant standards (width, spaces between the letters, and so on).
- Required fields and inscriptions.

- **Data extraction** (full name, home address, issue date).

- **Data validation** (whether the address is complete, if it exists and if it is really a home address).

To ensure the completeness and consistency of the extracted address data, external map services, such as Google Maps, Open Street Map, and others, are utilized allowing the MLCO to see the applicant's geolocation in the Dashboard.

(b) Supported PoA Documents

Common proof of residency examples:

- Tax bill (not older than 3 months).
- Mortgage statement.
- Certificate of voter registration.
- Correspondence with a government authority regarding the receipt of benefits such as a pension, unemployment benefits, housing benefits, and so on.
- Cable internet/TV bill (but not from satellite TV companies or for other wireless telecommunication services).
- Landline telephone bill.
- Bank statement with the date of issue and the name of the person (the document must be not older than 3 months).
- Utility bill for gas, electricity, water, internet, etc. linked to the property (the document must not be older than 3 months).
- A lease agreement that is current and has the signatures of the landlord and the tenant.
- Rent bills issued by a real estate rental agency.
- Credit card statement issued by a bank.
- Letter from a recognized public authority or public servant (any government-issued correspondence not older than 3 months).
- Employer's certificate for PoA.
- House purchase deed.
- The document must contain the full name, home address, and the document issue date (in most cases).
Electronic documents (in PDF) are accepted.

Alternative proof of residency examples

The following documents can also be accepted as valid PoA, but only if they contain an address:

- Passport
- Identity card
- Driving license
- Residence permit (EU samples containing address)

**** The same document cannot be used to confirm both an identity and a place of residence. So, if an applicant submits an ID document as PoA, they should use another document to confirm their identity.*

Documents which are not acceptable as Proof of Address, include:

- Old government-issued correspondence (older than 3 months)
- Old bank statements (older than 3 months)
- Old utility bills linked to the property (older than 3 months)
- Pension statements
- Bank references
- Insurance policies
- Mobile phone bills
- Medical bills
- Receipts for purchases
- Insurance statements
- Documents stating PO Box addresses
- Checks
- Envelopes and parcels showing your name and an address
- Prepaid card invoices
- Mobile sim cards+ bills issued to a business address
- Bills from debt collection agencies
- Bills from fintech companies
- Papers referring to discount cards which cannot be considered as bank cards
- Car rent bills

9. Payment card verification

The customer must provide a screen shot of the card showing the customer's first and last name, as well as a bank statement to confirm the payment.

10. Liveness Detection

The purpose of Liveness Detection is to ensure that an applicant is a real person (not a paper mask, a photo, a doll or something similar), not a duplicate and the holder of the account and documents which have been uploaded to the applicant profile. The Liveness check can be passed only if an applicant is awake and looking right into the camera. It also takes just four seconds to rotate one's head which streamlines onboarding and makes the process much more user-friendly.

Liveness Detection detects:

- Physical and digital images.
- Paper masks.
- Deepfakes, lookalikes, and doppelgangers.
- Masks, wax figures, and lifelike dolls.
- High resolution videos.
- Setting Up Liveness Check

11. Source of Funds (SoF) and Source of Wealth (SoW)

SoF refers to origin of funds being deposited, received, or transferred with the Company. SoF tells us where the money is coming from, which can be proven through bank statements, tax returns or the Company financials, etc.

Typically, SoW is requested when establishing business relationships or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

Examples of SoW and SoF and supporting documentation that can be provided, include:

Income category	Documents required
Income from salary	▪ Pay slips for the past 3 months and bank statement showing the salary being paid into this bank account; ▪ Audited personal tax statement.
Inheritance	▪ Grant of Probate (with a copy of the Will) clearly showing the amount of inheritance and a bank statement showing these funds being deposited into the account; ▪ Signed letter from a licensed solicitor or estate trustees on letter-headed paper clearly indicating the amount of inheritance, accompanied by updated proof of the solicitor's regulated status and a bank statement showing these funds being deposited into the account.
Gift/donation	▪ Notarized gift/ donation letter and a bank statement showing these funds being deposited into the account; ▪ Gift agreement and a bank statement showing these funds being deposited into the account.
Savings/deposits	▪ Savings statement; ▪ Bank statement.
Government grants (retirement income, grants for veterans, research grant, etc.)	▪ Type of received grant and a bank statement showing these funds being deposited into the account; ▪ Documents confirming/ proving received grant and a bank statement showing these funds being deposited into the account.
Company profit / dividends	▪ Dividend contract note or equivalent and a bank statement showing these funds being deposited into the account; ▪ Copy of latest audited financial statements; ▪ Tax declaration form.
Loan or investment	▪ Loan/Investment agreement or other documents confirming the agreement and a bank statement showing these funds being deposited into the account.
Sales (of property, goods, shares, etc.)	▪ Copy of contract of buy/sale/production and a bank statement showing these funds being deposited into the account; ▪ Prove of e-shop sale report (screenshot) with the list of items sold and a bank statement showing these funds being deposited into the account; ▪ Shipping documents and a bank statement showing these funds being deposited into the account; ▪ Proof of delivery and a bank statement showing these funds being deposited into the account; ▪ Customs declaration; ▪ Audited financial report; ▪ Tax report; ▪ PayPal statement evidencing the money and a bank statement showing these funds being deposited into the account.

ANNEX II - INDICATIONS OF AN UNUSUAL TRANSACTIONS

The list should not be considered as final but as minimal requirement and as indicative. All good practices and sources must be used to prevent money laundering and terrorist financing.

1. The following transactions or intended transactions are deemed unusual:
- (a) Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
 - (b) Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
 - (c) Transactions in the amount of NAf. 5,000 or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. This includes but is not limited to:
 - (c 1) A cashless transaction in the amount of NAf. 5,000 or more.
 - (c 2) A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
 - (c 3) Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
 - (c 4) Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits.
 - (c 5) A cash out in the amount of NAf. 5,000 or more;
 - (d.) Presumed money laundering transactions or terrorist financing: Transactions where there is cause to presume that they can be related to money laundering or terrorist financing.

Note: A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAf. 5,000.

ANNEX III - "INTERNAL SUSPICION REPORT"

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER

Name:	Tel: +
Dept:	Fax: +
Position:	e-mail:

CLIENT REPORTED

Full description and details of transaction/activity arising suspicion:

Reason for suspicion:

Other information that may be relevant:

SIGNATURE

DATE

TO BE COMPLETE BY MLCO

DATE RECEIVED:	_____
REF. NO. ASSIGNED:	_____
SIGNATURE:	_____

ANNEX IV - “INTERNAL EVALUATION REPORT”

INTERNAL EVALUATION REPORT
BY MLCO

Reference of Internal Suspicion Report	Client's Details:
Informer's Full Name	
Informer's Dept:	Client Agreement #:
Informer's Position:	Risk category:

Enquiries undertaken:

Documents attached and research performed:

MLCO's Decision:

MLCO Signature: _____	Date: _/ _/ _	Time: _____
-----------------------	---------------	-------------

ANNEX V – SANCTIONS POLICY

1. Background

The Company is obliged to comply with laws imposing financial and other restrictions on dealings with certain, entities, individuals and countries. This Sanctions Policy (hereinafter the “Policy”) sets out requirements and procedures designed to promote compliance with such laws (sanctions). Sanctions are a policy tool that national governments and multinational organisations use to constrain and deter perceived threats to their security, or to conform international conduct to recognised international standards. Sanctions arise in response to the conduct of countries, geopolitical rivals or transnational actors or trends. While national-level and multilateral sanctions regimes vary in content, rules, and restrictions, and the substance and frequency of enforcement action, they tend to fall into one of the below categories:

- **Comprehensive sanctions.** These sanctions target entire countries or geographic regions and prohibit most activity involving those countries or jurisdictions. Comprehensive sanctions aim to alter government behavior by imposing economy-wide costs, restricting access to arms and tools of internal repression, and restricting access to a wide range of goods and services.
- **Regime-based sanctions.** These sanctions target current (or former) governments or regimes. They are not comprehensive: although they are associated with particular countries, they are primarily list-based, focused on officials involved in activity deemed to be a threat to national security, economy, or foreign policy and on their associates. These sanctions tend to be paired with limited export controls or embargoes and related financing prohibitions. Most regime-based sanctions aim to protect human rights, combat state-sponsored or grand-scale corruption, and support democratic processes, institutions, and the rule of law.
- **Sectoral sanctions.** These sanctions target entities in a key sector or sectors of a country's economy. Importantly, they may still allow for many ordinary business transactions with the country at issue, even with respect to the listed entities. The listed entities may not be themselves involved in targeted activity, but they may be identified due to their relationship to government decision-makers (to exert pressure on those decision-makers) or because of their importance to a country's economy or future growth prospects.
- **Special debt and/or equity sanctions.** These relatively complex prohibitions allow for the continuation of day-to-day business with targeted entities while restricting the ability of targets to deal in new or new equity (valuable for, e.g., raising capital for long-term projects). These sanctions have generally been applied to entities within specific economic sectors (e.g., energy) but have also been applied to entities owned or controlled by a target government.
- **Conduct-based sanctions.** These list-based sanctions, as described in an additional resource, are directed not at particular countries or governments but rather at anyone involved in defined types of malicious activity. Persons and entities can be designated for involvement in terrorism, proliferation of weapons of mass destruction, bribery/corruption, human rights violations, drug trafficking, organized crime, election interference, and cyberenabled malicious activity. Conduct-based sanctions are meant to identify, disrupt, and deter sanctioned activities.

The key types of sanctions listed above may vary on the above characteristics even within a single category. Nor are these key types of sanctions mutually exclusive (e.g., regime-based sanctions may overlap with special debt and/or equity sanctions).

2. Policy Statement

Under this Sanctions Policy, the Company must:

- Where required by law, block accounts and other assets of sanctioned entities and individuals.
- In all other instances, prohibit or reject unlicensed trade and financial transactions with sanctioned jurisdictions, entities, and individuals.
- Exit relationships with Clients confirmed to be subject to sanctions, regardless of whether this is required by local law in the jurisdiction where the account or relationship is based.

- The Company must not knowingly engage in any transactions and/or business relationships structured to or aimed at the circumvention of applicable sanctions restrictions.

Failure to comply with this Policy may expose the Company to regulatory action or fines, civil or criminal liability as well as possible reputational damage.

3. Sanction Screening

The Company must ensure that sanctions screening is performed on existing and prospective Clients, connected parties, transactions and third parties against sanction lists.

The Company uses the services of the specialized third-party risk management **Sum and Substance Ltd** and ISPIRAL IT SOLUTIONS LTD to conduct screenings to identify potentially sanctioned persons/entities before establishing business relationships with them.

Sum and Substance Ltd is registered with the Information Commissioner's Office in line with the Data Protection Act 2018. Additionally, Sum and Substance Ltd has obtained the following certifications and attestations:

SOC 2 Type 1	SOC 2 Type 1 examination, which was proctored by independent auditor BARR Advisory, P.A. This assessment confirms that Sumsb has rigorous security controls against unauthorized access, disclosure or damage of data.
ISO/IEC 27001	This standard covers the security of development, implementation, functioning, monitoring, analysis, support and improvement of Sumsb's ISMS (Information Security Management System), which is audited on an annual basis.
ISO/IEC 27017	This certification demonstrates that Sumsb adheres to technical and organizational measures regarding risk assessments, equipment, software controls, personnel work, the backup procedure and other processes related to cloud service security.
ISO/IEC 27018	This certificate confirms that Sumsb has commonly accepted control objectives and guidelines for implementing measures to protect Personally Identifiable Information (PII) privacy principles in the public cloud computing environment.
PCI/DSS	The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from major card schemes. This certification confirms that Sumsb is fully compliant with high standards for secure storage and processing of bank card data.

The specialized third party risk management solution selected by the Company shall ensure **ongoing** sanction screening process after a business relationship is established. The potentially matching data from various sanctions and watchlists is compared against the applicant profile to establish an exact match, before a match status is assigned. The following types of status may be assigned:

True positive: Applicant data exactly matches one or several watchlist records.

Potential match: Name of the applicant matches one or several watchlist records, but the age/year of birth data is missing or the applicant is suspected of committing a crime.

False Positive:

- Applicant data does not match any of the watchlist records.
- Applicant data matches the watchlist record exactly, but additional information clearly shows that the applicant and the person on the record are different people.
- Applicant data matches the watchlist record, but the record does not include criminal or suspicious information about a person. For example, if the applicant is a crime journalist, and their name features on the article as the author.

Unknown: Applicant name in the document contains only one word.

Applicants with “True Positive” and “Potential Match” statuses are delegated to the MLCO for further processing. If applicants are declined based on a watchlist match, they are assigned a respective rejection tag:

- Sanctions
- PEP
- Criminal records
- Adverse Media

-In case of positive matches against sanctions lists, the action performed by the MLCO will be in line with the requirements of a specific sanctions program (e.g. asset freeze, rejection, etc.) as well in consideration with any potential conflict of law.

4. Asset Freezing

For the purpose of this Policy, freezing, also known as “blocking”, refers to a form of controlling assets in which a sanctioned party has an interest. While title to blocked property remains with the sanctioned party, the exercise of the powers and privileges normally associated with ownership is prohibited without authorisation from the sanctioning competent authority. Blocking immediately imposes an across-the-board prohibition against transfers or transactions of any kind with regard to the property.

“Assets” refer to tangible or intangible resources with economic value that an individual, corporation or country owns or controls with the expectation that it will provide future benefit. In case of the Company, the assets include cryptocurrency and fiat currency.

Where required by the applicable sanctions laws and regulations, the MLCO must perform the freezing of assets. The Company must have a separate account for frozen funds and send a report to the FIU.

5. Outsourcing

Where a sanctions compliance activity is outsourced to an entity outside the Company, the Company is ultimately accountable for ensuring that such activities are undertaken in compliance with the requirements of this Policy, and all applicable sanctions laws, rules and regulations.

6. Record-Keeping And Record Retention

The Company adopts one set of record-keeping and record retention rules and requirements to all sanctions-related items as set by the Company’s AML Policy.

ANNEX VI - REGISTRY OF TERMINATED TRANSACTIONS AND/OR THE BUSINESS RELATIONSHIPS

No.	Date of entry	Client (natural person)				Beneficial owner				Termination reason
			Natural person							
		Given name, surname	Date of birth	Personal ID number (if has)	Nationality	Given name, surname	Date of birth	Personal ID number	Nationality	

ANNEX VII – Country (Excell form)