Precise IG Solutions B.V.
Registration number: 162989
Schottegatweg Oost Unit 1-9 Bon Bini
Business Center, Curacao

Money Laundering and Terrorism Financing Prevention Policy

Last update: 19th of May 2023
Approved by the Director
Date: 19th of May 2023

1. General provisions

1.1. The Money Laundering and Terrorist Financing Prevention Policy (the "**Policy**") establishes the procedure for implementation of the requirements laid down in Curacao Laws related to Prevention of Money Laundering and / or Terrorist Financing (the "**Laws**") of Precise IG Solutions B.V., registration number 162989, registered at Schottegatweg Oost Unit 1-9 Bon Bini Business Center, Curacao (the "**Company**").

1.2. The Company's main business is to provide online gaming (gambling) services.

1.3. This Policy applies to the Company in cases when the Company's customers seek to establish a business relationship with the Company, as well as to implement ongoing monitoring of Company's customers' business behavior and is applied to ensure safety and transparency of both customers and Company's funds. Employees of the Company whose responsibilities are related to prevention of money laundering and terrorist financing or outsourced service providers are responsible for the implementation of this Policy.

1.4. Company's customers - natural persons who in order to become a customer of the Company apply for the creation of an account on the Company's website https://coinpoker.com/ (or associated Company's websites) or app (the "**Customer**").

1.5. This Policy is in line with Curacao legislation on the Prevention of Money Laundering and Terrorist Financing (National Ordinance on identification when rendering services and the National Ordinance on the reporting of unusual transactions) also recommendations of the Financial Action Task Force on Money Laundering and Terrorist Financing (FATF) and Caribbean Financial Action Task Force (CFTAF) and other documents.

1.6. Implementation of anti-money laundering and/or terrorist financing measures compliance to anti-money laundering and/or terrorist financing requirements are supervised by The Curacao Gaming Control Board and (official website: www.gamingcontrolcuracao.org) (the "**Supervisory authority**") and Cyberluck Curacao N.V. (the "**Supervisory authority**").

1.7. The Company will provide services in virtual and fiat currencies. All fiat currencies that will be available to deposit for provision of services, hereinafter are referred as (the "**Funds**") and policy is applicable only to transactions executed in fiat currencies..

2. Risk-based approach

2.1. The nature of the services provided by the Company poses a significant risk of money laundering and/or terrorist financing, therefore the Company's Customers also pose a risk to be involved in money laundering and/or terrorist financing activities or may use the Company as tool for money laundering and/or terrorist financing.

2.2. Due to the risks indicated in point 2.1. of the Policy, the Company based on the identity of the Customer and Customer's risk characteristics specified in this Policy, classifies Customer to one of the following risk categories:

2.2.1. Low Risk Customer;
2.2.2. Medium Risk Customer;
2.2.3. High Risk Customer;

2.3. During the process of onboarding the Customer, the Company has to perform identification of the Customer and implement specific measures (checks) based on which the Customer is classified to one of the risk categories listed in points 2.2.1.-2.2.3. of this Policy. The risk factors due to which specific measures are implemented are as follows:

2.3.1. The Customer is involved in adverse media, i.e., negative news in the media is linked to the Customer (related with terrorism, financial crimes, violence, narcotics, cybercrime, fraud, etc.);
2.3.2. The Customer is considered as politically exposed person (PEP);
2.3.3. The Customer is listed on a sanction's lists (restrictions imposed on individual);
2.3.4. Geographical Customer's location is considered as a high-risk country and jurisdictions under Increased Monitoring as indicated by FATF.

2.4. The Customers are classified by default as Low Risk Customer until the moment when the Company implement specific measures (perform checks) and classifies the Customer to each risk category. The Customers shall be classified as follows:
2.4.1. Low Risk Customer – none of the factors listed in points 2.3.1.-2.3.4. of the Policy are applicable to the client;
2.4.2. Medium Risk Customer – the Customer matches no more than one of the factors listed in 2.3.1.-2.3.4. of the Policy;
2.4.3. High-Risk Customer – the Customer matches at least two of the factors listed in 2.3.1.-2.3.4. of the Policy;

2.5. The Company shall apply respective Enhanced Due Diligence (EDD) measures to Medium Risk Customers. In case the Company decides to not apply Enhanced Due Diligence (EDD) measures to Medium Risk Customers, the Company notice Customer regarding decision not to establish business relationship.

2.6. The Company does not establish a business relationship with the Customer if the Customer is classified as a High-Risk Customer.

3. Identification of the Customer. Establishment of business relationship

3.1. The identity of the Customer (beneficial owner) in the Company is established only remotely. Once the Customer has been identified, the identity of the beneficial owner shall be deemed to be identified as well.

3.2. By signing up and applying for the account opening in the Company, the Customer fills-in online application by indicating his / her personal data as follows:
3.2.1. Full legal name of the Customer;
3.2.2. Date of birth of the Customer;
3.2.3. Full address of the Customer;
3.2.4. Contact details (phone number and email address) of the Customer;

3.3. For Customers identification purposes, the Company requests from Customers to upload and provide proof of identity documents together with address proof documentation to verify their account opened with the Company when the following conditions are met:
3.3.1. When Customer deposits any amount of Funds in his/her account opened with the Company;
3.3.2. When Customer proposes to withdraw Funds from the account opened with the Company.

3.4. The Company only considers provided documentation from the Customer suitable if scanned copies and / or good quality photos are provided to the Company.

3.5. Uploaded and provided proof of identity and address proof documents are verified and full name is compared, if full name provided during sign-up matches name of the provided proof of identity document the identity of the Customer is verified.

3.6. The following identity proof documents are acceptable for verifying identity and address of the Customer:
3.6.1. Copy of national ID card, passport or driving license;
3.6.2. Copy of utility bill (not older than 6 months);
3.6.3. Copy of bank statement (not older than 6 months);
3.6.4. Any other proof document which is requested by the Company on an individual case.

3.7. In cases when the Company receives proof of identity and address proof documents from Customers and information/details in the provided identity and address proof documents are different than details in provided filled online application form in the sign-up process – Customer account opened with the Company is closed and business relationship with the Customer is terminated. Also, in cases when the Company receives filled online application and personal proof of identity documents of the Customer and determines that the Customer is underaged (under age that gambling or gaming activities are legal under the law or jurisdiction that applies to Customer) and/or is prohibited to participate in gambling activities (listed on register of persons restricted from participation in gambling) the Company immediately notice Customer regarding decision not to establish business relationship. Respective record is made in the register of terminated business relationship.

3.8. The Company requests to be provided with suitable documents once again and until provided cannot verify the Customer's identity in cases as follows:

3.8.1. the Customer did not provide any of required documents confirming his identity;

3.8.2. the Customer did not provide all required documents or provided documentation was incorrect/unrelated with the data indicated in online application;

3.8.3. the documents were not provided in conformity to points 3.4. and 3.6. of this Policy.

3.9. All data and documents of the Customer collected during stage of the Customer's identification indicated in section 3 of this Policy shall be recorded and stored in accordance to point 9.3. of this Policy.

4. Risk-based evaluation of the Customer

4.1. Once the Customer has been identified in accordance to the procedure indicated in point 3.2. of this Policy, the Company shall apply risk-based approach.

4.2. The Company perform the Customer's risk-based evaluation in accordance to the personal data of the Customer indicated in the filled online application and provided documents and implement specific measures (perform checks) in order to find out if the Customer meets the risk factors in points 2.3.1.-2.3.4. of the Policy.

4.3. Risk-based evaluation of the Customer is performed by using publicly available information / tools and other reliable and independent sources or service providers. The Company shall use publicly available sources as follows: www.google.com, http://www.sanctionssearch.ofac.treas.gov, http://www.dilisense.com/ and other alternative websites or databases from services providers. Key words as bribery, laundering, fraud etc. Shall be used during checks of the Customer.

4.4. All data of the Customer collected during stage of the Customer's risk-based evaluation indicated in section 4 of this Policy shall be recorded and stored in accordance to point 9.3. of this Policy.

4.5. In case none of the risk factors applied to the Customer – meaning that the Customer is classified as the Low-Risk Customer – the Company decides to establish business relationship with the Customer. The decision to establish a business relationship is expressed by making a record in the Company's register of establishment of a business relationship with Customers. Following the decision to establish a relationship with the Customer, the Company while providing services continues to perform ongoing due diligence of the Customer, periodic reviews of the relevance of the data and notices the Supervisory authority about unusual/suspicious activity.

5. Enhanced Due Diligence of the Customer

5.1. In cases when results of risk-based evaluation indicates that no more than one the risk factor applies to the Customer – meaning Customer was classified as Medium Risk Customer – the Company shall perform Enhanced Due Diligence (EDD) of the Customer. The Company is entitled to adopt decision not to perform Enhanced Due Diligence (EDD) of the Customer as indicated in point 2.5. of this Policy. In cases when at least two of the factors listed in 2.3.1.-2.3.4. of the Policy apply to the Customer – meaning Customer was classified as High-Risk

Customer – the Company notice Customer regarding decision not to establish business relationship. Respective record shall be made in the register of terminated business relationship.

5.2. By performing Enhanced Due Diligence (EDD) of the Customer, the Company implements measures to eliminate risk of money laundering and/or terrorist financing as follows:
  5.2.1. obtaining additional information/explanation and/or documents from the Customer;
  5.2.2. obtaining the approval of senior manager of the Company for establishing the business relationship;
  5.2.3. obtaining information and/or documents on the source of funds and source of wealth of the customer;
  5.2.4. any other data/information that employees of the Company considers relevant to eliminate or mitigate the risk.

5.3. If the Customer avoids to provide above mentioned explanations/information and/or documents or provided explanations/information and/or documents do not allow to mitigate the risk of money laundering and/or terrorist financing, the Company notice Customer regarding decision not to establish business relationship.

5.4. In cases when Customer provides requested information/explanation and/or documents and provided information/explanation and/or documents allows to eliminate or mitigate the risk of money laundering and/or terrorist financing, the Company decides whether to establish or not business relationship with the Customer.

5.5. The Company's decisions to or not to establish business relationship after performance of Enhanced Due Diligence (EDD) shall be expressed by making a record in the Company's register of establishment of a business relationship with Customers or register of terminated business relationship. Following the decision to establish a relationship with the Customer, the Company while providing services continues to perform ongoing due diligence of the Customer, periodic reviews of the relevance of the data and notices the Supervisory authority about unusual/suspicious activity.

5.6. All data of the Customer collected during stage of Enhanced Due Diligence (EDD) of the Customer indicated in section 5 of this Policy shall be recorded and stored in accordance to point 9.3. of this Policy.

6. Ongoing Due Diligence

6.1. While providing services, the Company shall continue to perform ongoing monitoring of the Customer, periodic reviews of the relevance of the data and informs the Supervisory authority about possible suspicious activity.

6.2. The Company must ensure continuous monitoring of Customers transactions and behavior to identify unusual operations or activities. Unusual indications may be related to the deposits made into Customer's account opened with the Company, abuse of bonuses or other promotions, using unfair external factors or influences, taking unfair advantage, opening any duplicate accounts with the Company, undertaking fraudulent practice or criminal activity, etc.

6.3. The Company shall ensure that the data, documents and information about the Customer are constantly updated (at least once every 24 months). In cases Enhanced Due Diligence (EDD) applied to the Customer during onboarding stage, data, documents and information shall be updated at least once every 12 months.

6.4. If the Customer avoids to submit updated documents, information and other data required by the Company within the reasonable time, the Company might terminate business relationship with the Customer. Even if the Customer provides requested information, decision to terminate or continue business relationships with the Customer is at the discretion of the Company and shall be made in accordance with any potential risk factors indicated in point 2.3.1.-2.3.4. of this Policy. Respective decision of the Company shall be expressed by making a record in the Company's register of termination of a business relationship with Customers or register of continued business relationship with Customers.

6.5. All data of the Customer collected during stage of Ongoing Due Diligence of the Customer indicated in section 6 of this Policy shall be recorded and stored in accordance to point 9.3. of this Policy.

7. Recognition, documentation and reporting of unusual/suspicious transactions

7.1. An unusual transaction shall be considered a transaction which is inconsistent with the Customer's business behavior or personal activities.

7.2. The Company shall pay special attention to all complex, unusually large transactions and all unusual patterns of transactions, which have no apparent economic or visible lawful purposes.

7.3. To guard against money laundering and/or terrorist financing the Company shall record any suspicious/unusual transaction in writing by making a record in the Company's register of unusual/suspicious transactions of the Customer. Such findings shall be kept of at least five years and shall be available for respective Curacao supervisory authorities.

7.4. In case unusual/suspicious transaction was detected and recorded, the senior manager shall be internally reported regarding this matter within undue delay, in the manner approved by the Company. Together with internal unusual/suspicious report senior manager shall be provided with all collected data related with the Customer being reported.

7.5. In cases when senior manager had evaluated nature, risks and other relevant circumstances of the transaction and authorized received report, external report shall be prepared and submitted to Supervisory authority without undue delay.

7.6. If the unusual transaction is not authorized by senior manager to be incorporated and reported to Supervisory authority, all documents relevant to the transaction including reasons for non-authorization shall be documented, undersigned by senior manager and kept for internal records in accordance to point 9.3. of this Policy.

7.7. The Company shall appoint a Money Laundering Reporting Officer (the "**MLRO**") who as the Non-Executive Director shall be responsible for the filing of a Quarterly preformatted Report, pertaining a risk analysis on Money Laundering (the "**MLR**") with the designated authorities.

7.8. The Executive Director shall be responsible for the drafting of the MLR and shall timely present a properly filled out MLR to the MLRO for approval and filing with the authorities in accordance to point 7.7. Both the Executive Director and Non-Executive Director are required to sign the MLR prior to its filing.

7.9. Notwithstanding anything to the contrary as referenced in point 7.7., the MLRO shall also be responsible for ensuring that, when appropriate, the information of any other matter leading to knowledge or suspicion, or reasonable grounds for knowledge or suspicion of Money Laundering is properly disclosed to relevant the authority.

7.10. The Report in accordance to point 7.7. shall at minimum include the following information:
(i) a general description of the policies on AML that have been implemented, including any updates or material changes;
(ii) any suspicions on Money Laundering;
(iii) any Incidents.

7.11. Whenever events transpire in accordance to the point 7.10. (ii) and (iii) the MLRO shall, in exception to the point 7.7. directly report such events to the designated authorities.

8. Employees training

8.1. The Company provides anti-money laundering/terrorism financing risk awareness training for employees. The Company intends to conduct trainings so frequently so Company's employees would be well familiarized with latest AML/KYC practices

8.2. Regardless of who conduct the employees training (senior manager or external providers) employees shall be instructed about the following matters:

8.2.1. obligations under Curacao anti-money laundering/terrorism financing laws and FATF, CFATF recommendations;
8.2.2. the consequences of not complying with anti-money laundering/terrorism financing requirements;
8.2.3. the types and patterns of money laundering and/or terrorism financing that the Company's business or organization might face and the consequences of these risks;
8.2.4. the Company's compliance to anti money-laundering/terrorism financing laws, including the Company's processes and procedures to identify, manage and mitigate risks related to money laundering/terrorism financing.

8.3. Anti-money laundering/terrorism financing risk awareness training programs to all employees, director(s) of the Company shall be conducted by senior manager. Aforementioned programs to senior manager shall be conducted by external providers.

8.4. Types of training, detailed training programs and its frequency shall be specified in the internal policies of the Company.

8.5. The Company ensures that Customers identifications of their identity or monitoring of their operations will be conducted by professional, well trained Company's employees.

9. Storage of registers and Customer's data

9.1. The Company shall maintain and store registers as follows:
9.1.1. register of establishment of business transactions;
9.1.2. register of continued business transactions;
9.1.3. register of terminated business transactions;
9.1.4. register of unusual/suspicious transactions.

9.2. The registers referred to in point 9.1. of the Policy shall be stored in electronic format for 5 years from the date of termination of business relations with the Customer.

9.3. All information/explanation, data and documents related with the Customer shall be stored in electronic format for 5 years from the date of termination of business relations with the Customer.

9.4. The Company shall keep secure all data given by the Customer shall not sold or give to anyone else. The data may only be shared with the AML authority of the affected state if forced by law, or to prevent money laundering.

10. Final provisions

10.1. This Policy is approved by the Company's Director. The Policy shall enter into force on the date of its approval, unless otherwise specified. The Company's Policy is reviewed regularly, but at least once a year and in case any adjustments are required, the new version of the Company's Policy takes effect from the date of its approval.