NOWPAYMENTS

INTERNAL RULES OF PROCEDURE

FOR

PREVENTION OF MONEY LAUNDERING

AND TERRORIST FINANCING

(AML AND KYC/KYB POLICY)

TABLE OF CONTENT

CUSTOMER IDENTIFICATION AND VERIFICATION (CUSTOMER ON-

1. GENERAL PROVISIONS

1.1 NOWPayments Ltd., a company duly organized under the laws of Seychelles (**"the Company"**), is committed to the highest standards of the Anti-Money Laundering (AML) compliance and Anti-Terrorist Financing, requires its management and employees to follow the named standards and actively prevents any actions that aim or facilitate the process of legalizing of illegally gained funds.

1.2 The internal rules of procedure for prevention of money laundering and terrorist financing (**"Rules"**) lay down internal security measures for conducting due diligence and detecting suspicious and unusual behavior in all areas of activity of our Company. All relevant employees should know and strictly follow the best AML/CFT standards as well as these Rules.

1.3 A copy of these Rules shall be available to all relevant employees of the Company.

2. DEFINITIONS

2.1 What is money laundering?

Conversion or transfer of property derived from criminal activity, or, property obtained instead of such property, knowing that such property is derived from criminal activity, or, from an act of participation in such activity, for the purpose of concealing, or disguising the illicit origin of the property, or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's actions.

- The acquisition, possession or use of property derived from criminal activity, or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein.
- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.

2.2 What is terrorist financing?

The allocation or raising of funds to plan or perform acts which are deemed to be acts of terrorism or to finance operations of terrorist organisations, or in the knowledge that the funds allocated or raised will be used for the aforementioned purposes.

2.3 What is a risk country?

Countries or regions of interest where the risk of money laundering or terrorism are high. A risk country is a country or jurisdiction that:

a. According to credible sources such as mutual evaluations, detailed evaluation reports or published follow-up reports, has not established effective AML/CFT systems;
b. According to credible sources, there has significant levels of corruption or other criminal activity;
c. Is subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
d. Provides funding or support for terrorist activities, or that has designated terrorist organisations operating within their country, as identified by the European Union or the United Nations.

2.4 What is a high-risk country?

A country which is according to the FATF is considered to be a high risk or a country specified in a delegated act adopted on the basis of Article 9(2) of Directive (EU) 2015/849 of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The current list is available here:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R1675-20181022

2.5 Who is a politically exposed person (PEP)?

A natural person who performs or performed prominent public functions as well as their family members and close associates. Persons who, by the date of entry into a transaction, have not performed any prominent public functions for at least one year, as well as their family members or close associates shall not be considered politically exposed persons.

For the purposes of these Rules of Procedure, the following persons shall be persons performing prominent public functions:

a. State, head of government, minister and deputy or assistant minister;
b. a member of parliament or of a similar legislative body, a member of a governing body of a political party, a member of a supreme court, a member of a court of auditors, or of the board of a central bank;
c. an ambassador, a chargé d'affaires or a high-ranking officer in armed forces;
d. a member of an administrative, management or supervisory body of a State-owned enterprise;
e. a director, deputy director or member of the board, or equivalent function, of an international organisation, except middle-ranking or more junior officials.

The following persons are considered family members of a person performing prominent public functions:

a. the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or a local politically exposed person;
b. a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person or local politically exposed person;
c. a parent of a politically exposed person or local politically exposed person.

The following persons are considered close associates of a person performing prominent public functions:

a. a natural person who is known to be the beneficial owner or to have joint beneficial ownership of a legal person or a legal arrangement, or any other close business relations, with a
politically exposed person or a local politically exposed person;
b. a natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person or local politically exposed person.

2. 6 Who is a Compliance Officer?

Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a compliance officer.

2.7 Who is a customer?

A legal entity which is partnered with the Company and to whom the Company provides its services.

2.8 Who is a relevant employee?

A person who is conducting KYB/AML measures about the customer in the Company.

2.9 What is a business relationship?

For the purposes of these Rules, a business relationship is a continued contractual relationship with a customer.

2.10 Who is the ultimate beneficial owner of a legal entity (UBO)?

Ultimate beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal entity or arrangement. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control. This definition should also apply to beneficial owners or a beneficiary under a life or other investment-linked insurance policy.

An UBO is a private individual owning or controlling more than 25% of a legal entity.

3. CUSTOMER IDENTIFICATION AND VERIFICATION (CUSTOMER ON-BOARDING)

3.1 The Company has the right to identify customers who want to use the Company's services (regardless of whether the customer is a regular customer or not) and ask them to finish a verification procedure.

Individual customers

3.2 For using the Company's services, the Company has the right to ask personal information from its customers, specifically:

Information collected	Purpose of collection of data
full name of the customer	● to provide the Company's services; ● to resolve the customer's claims; ● to communicate with the customer.
date of birth of the customer	
customer's e-mail	
origin of the customer (customer's place of residence)	
address of the customer's payment wallet	

3.3 The Company has the right to identify the customer based on the following information:

- proof of identification (high-resolution copy of an identity card, passport, diplomatic passport, or driving license - if the document shows the full name, photo or face image, signature of its holder and the date of birth);
- proof of residence (high-resolution copy of an utility bill of the customer, tax document or bank reference - these documents should not be older than three (3) months from the date of filing);
- if the customer is in fact representing another private individual being the real customer (under a power of attorney, or in the case of inheritance, or any other way) information on the identification and verification of the right of representation and scope thereof and, where the right of representation does not arise from law, the name of the document serving as the basis for the right of representation, the date of issue, and the name of the issuer.

Corporate customers

3.4 If the customer is a legal entity, the Company has the right to ask it to provide:

Information collected	Purpose of collection of data
legal name of the customer	● to provide the Company's services; ● to resolve the customer's claims; ● to communicate with the customer.
date of incorporation of the customer	
customer's e-mail	
origin of the customer (customer's place of residence)	
address of the customer's payment wallet	

3.5 The Company has the right identify the customer based on the following information:

- a high-resolution copy of the certificate of incorporation (an extract from the Commercial Register or equivalent document, evidencing the registration of the corporate customer);
- names and addresses of all directors and beneficial owners of the corporate entity.

3.6 The Company must identify the beneficial owners (UBOs) and, for the purpose of verifying their identities, taking measures to the extent that allows the Company to make certain that it knows who the beneficial owners are, and understands the ownership and control structure of the corporate customer, or of the person participating in the transaction.

3.7 If the customer of the Company provides financial services, the customer shall provide the AML letter to the Company. AML letter shall describe the AML/KYC measures the customer has applied in its services.

3.8 A representative of the corporate customer must submit a document certifying his/her powers (a power of attorney), which has been authenticated by a public notary and/or legalized and/or certified with an apostille, unless otherwise provided for in an international agreement.

3.9 Where the original document specified in this section is not available, the identity can be verified on the basis of a document specified in this section, which has been authenticated by a notary or certified by a notary or officially, or on the basis of other information originating from a credible and independent source, including means of electronic identification.

3.10 The Company verifies the correctness of the data, using information originating from a credible and independent source for that purpose. The Company may use available online databases to verify the information about the customer.

3.11 The Processing Provider may ask for additional information about the customer in case of any suspicion about the customer's identity information or the customer's behavior. Such additional information asked should be relevant to the raised risks which, when obtained, may prove that the risks are in fact explainable.

3.12 The Processing Provider may cross-check the customer through appropriate sanctions lists including but not limited to:

- OFAC SDN
- United Nations Security Council Sanctions List
- World Bank - Ineligible Firms And Individuals List
- EU - Financial Sanctions List
- UK - HMT Financial Sanctions List
- AU - DFAT Consolidated Sanction List
- US - Bureau Of Industry And Security List
- CH - SECO Sanction List
- US - Department Of State Nonproliferation Sanctions List
- Interpol Wanted List

4. ENHANCED DUE DILIGENCE

4.1 The Processing Provider can undertake enhanced due diligence (EDD) if there is a higher risk of money laundering or terrorist financing such as:

a. there are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner;
b. the customer is a politically exposed person (except for a local politically exposed person, their family members or a close associates);
c. the customer is from a high-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country;
d. the customer is from a Risk country, or from a territory that is considered a low tax rate territory.

4.2 Other factors that are referring to a higher risk pertaining to the customer:

e. When there are unusual factors in the customer onboarding;
f. Customer is a legal person or a legal arrangement, which is engaged in holding personal assets;
g. The customer is a company that has nominee shareholders or bearer shares or a company whose affiliate has nominee shareholders or bearer shares;
h. The ownership structure of the customer company appears unusual or excessively complex, given the nature of the company's business.

4.3 Other factors that are referring to a higher risk pertaining to the product, service, transaction or delivery channel:

i. Products/services that favours anonymity;
j. Payments received from unknown or unassociated third parties.

4.4 The Provider can identify what the risks are in every particular case and undertake all appropriate measures to mitigate those risks. Depending on the case, the Processing Provider may apply one or several of the following due diligence measures:

k. verification of information additionally submitted upon identification of the customer based on additional documents, data or information originating from a credible and independent source;
l. gathering additional information on the purpose and nature of the business relationship and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source;
m. making of the first payment related to a transaction via an account that has been opened in the name of the customer participating in the transaction in a credit institution registered or having its place of business in the European Economic Area or in a country where requirements equal to those of Directive (EU) 2015/849 of the European Parliament and of the Council are in force.

5. INTERNATIONAL SANCTIONS

5.1 The Company is prohibited from transacting with companies and countries that are on prescribed sanctions lists. The Company will therefore screen its customers against international sanction lists on a periodical basis

5.2 The Processing Provider can draw special attention to the Company's customer (present and new) and to the facts which refer to the possibility that the customer is a subject to International Sanctions. The customer, its representative, directors and UBOs must be checked against the international sanctions.

5.3 The customer can be checked against the international sanction on the website provided by the FMS or using other databases.

6. DATA COLLECTION AND RECORD-KEEPING

6.1 The Company is obliged to keep all records about the customer in such a way that it can always be presented on a legal request.

6.2 The Compliance Officer is responsible for keeping all relevant data.

6.3 The personal data of a customer, a customer's transaction and other relevant information must be stored for no less than 5 years after termination of the business relationship.

7. RISK BASED APPROACH

7.1 The relevant employee analysing the customer and his/her behaviour should undertake investigative efforts that are proportional to the risk and complexity of the case and collect evidence using observations gathered in the case.

7.2 If the relevant employee identifies any additional risks, they will need to conduct investigative research to understand these risks in the context of the case.

8. RISKS RELATING TO NEW AND EXISTING TECHNOLOGIES

8.1 The Company understands the risks that may come from new and existing technologies such as to fake location, to fraud the service, to corrupt the verification process.

8.2 The Company shall constantly audit its services for compliance with the best AML framework and technical standards to be sure the customer usage of the Company's service is secure and reliable for any corrupt activities.

8.3 The Compliance Officer monitors, identifies threats and reports to the management board.

9. INTERACTION WITH THE CUSTOMER

9.1 The relevant employee may contact the customer to clarify the information given or ask for additional information which is needed for the customer identification, or to address the risks of the case.

9.2 The relevant employee should not request unnecessary or irrelevant information. A request for additional information must be related to the risks of the case that after the customer's response, the relevant employee may close or report the case to the Compliance Officer. If the risk of money laundering or terrorist financing is very high, the relevant employee shall report the case to the Compliance Officer without asking additional information from the customer.

9.3.The relevant employee shall endeavor to never express themselves using words that give a reason for the customer to understand that his/her activity is suspicious and may be a subject for further report to the Compliance Officer.

10. MONITORING BUSINESS RELATIONSHIP

10.1 The Company shall monitor information on the customer on an annual basis.

10.2 If the Company has reasons to believe that the customer's information submitted upon onboarding has changed, the Customer shall require additional and up-to-date information.

11. MONITORING THE TRANSACTIONS

11.1 A transaction monitoring case may be initiated based on a behaviour trigger of the customer or manually by the Processing Provider. The Processing Provider has the right to investigate every initiated case.

11.2 The Processing Provider should determine what the risks of the case are. Each risk should be addressed and documented.

11.3 The Processing Provider has the right to conduct a pre-research and check whether the customer was checked previously and what were the concerns earlier

11.4 The Processing Provider has the right to conduct customer research to determine the customer's profile and identify the source and origin of the funds used in a transaction.

11.5 The Processing Provider can conduct an activity research of the customer and determine whether it is in line with the customer profile or if the behaviour seems suspicious. Activity research may include all observations about the customer's behaviour and any red flags in the activity.

11.6 The Processing Provider has the right to conduct research on all the counterparties if it is applicable in the case.

11.7 The case review may vary on the evidence needed to collect about the customer and his/her activity. The Processing Provider should use a risk-based approach to address the risks proportionally.

11.8 The Processing Provider can document all the findings about the customer and customer's behaviour which support the decision of the Provider about closing.

12. RISK APPETITE AND PEP's REQUIREMENTS

12.1 In order to allow a PEP (except the local PEP) to be the customer, the following must be fulfilled:

a. An approval from our company's management board for establishing a business relationship with that person.

b. Take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship.
c. Where a business relationship is entered into, conduct enhanced ongoing monitoring of the relationship.

12.2 Every customer is checked against the PEP database.

12.3 If the relevant employee does not use the outsourcing partner for checking the PEP status, the relevant employee should use generally known internet research engines and the databases the Company has access to.

12.4 The relevant employee should make a research using the potential customer's full name. In case, there are several similar results, the relevant employee must use another identifier (date of birth etc.) to be sure that the result found matches with the potential customer.

12.5 **The relevant employee shall refuse to onboard the customer and report to the Compliance Officer in case the relevant employee finds out that:**

d. **the customer is accessing the service from the high-risk country according to the EU or FATF list;**
e. **the customer is under sanctions in Georgia, the European Union or USA;**
f. **the customer is known to be accused with money laundering or terrorist financing;**
g. **the customer refuses to provide information requested by the Company;**
h. **the customer is acting on behalf of a third party who is considered to be an ultimate beneficiary.**

13. RISK ASSESSMENT

13.1 The customer may be assigned a risk score based on information gathered under the Rules for a customer.

13.2 The Company's policy is to work with low and normal risk customers. However, the customer's risk score may be changed in time due to change of the customer's behavior and/or customer information. Therefore, the Company may appear to work with high risk customers. Depending on the risk score of the customer, the Company applies the following risk categories:

- **LOW RISK**

a. The customer is considered to be a lower risk if the Company has internal information about the trustworthiness of the customer and his/her reasonable behaviour collected during a long commercial relationship.

- **NORMAL RISK**

The customer is considered to be a normal risk if:

a. There are no circumstances regarding the customer that indicate the presence of high or low risk in this category.
b. The customer has a legitimate reason why he/she cannot provide reliable evidence of his/her identity. For example, if he is an asylum seeker.
c. The customer uses the services and goods selected in the course of the business relationship in the expected manner.

- **HIGH RISK**

The customer is considered to be a high risk if:

a. The customer or representative of the client is the PEP, relative or close associate of such a person.
b. The customer has strong ties with senior government officials.
c. There is a presence of negative information in the media or in other relevant sources regarding the customer.
d. The property of the customer or the property of its publicly known close associate was frozen during the proceedings on charges of terrorism or the financing of terrorism.
e. There is a presence of past notifications of suspicious transactions involving a customer.
f. The Company has suspicions about the correctness and accuracy of customer identification.
g. The customer tries to avoid creating a commercial relationship, although this would be economically feasible and more logical.
h. The customer uses the services and goods selected during the course of the business relationship in an unexpected manner.

13.3 When establishing the risk category of a customer, the country of incorporation of the customer and status of PEP shall be taken into account.

13.4 If there are several characteristics of the category Higher Risk present, the Company shall address each of that risk.

Some characteristics of high risk and the appropriate due diligence measures (the list is not exhaustive):

Higher Risk	**Due Diligence Measures**
The customer is a politically exposed person (except for a local politically exposed person, their family members or a close associates);	The decision is taken by the MB.
There is information that the customer is suspected to be or to have been linked with a financial offence or other suspicious activities.	Check customers against International Sanctions or adverse information. Make a search on the customer in open databases or on the Internet. Ask guidance from the Compliance Officer

There are doubts as to the truthfulness of the submitted data, authenticity of the documents or identification of the beneficial owner	Conduct an internet search about the customer.. Ask for additional information which proves the authenticity of the documents. If there are no other circumstances leading to the higher risk and the MB approves, it is not required to apply EDD measures stipulated in Section 4
The customer is from a High-risk third country or their place of residence or seat or the seat of the payment service provider of the payee is in a high-risk third country	Seek guidelines from the Compliance Officer.
When there are unusual factors in the customer onboarding, or when there are unusual transactions patterns without clear economic or lawful purpose	Conduct an internet search about the Client. Collect additional information on the purpose and nature of the business relationship, transaction or operation and verifying the submitted information based on additional documents, data or information that originates from a reliable and independent source
The customer or the person using the professional service is from such country or territory or their place of residence or seat or the seat of the payment service provider of the payee is in a country or territory that, according to credible sources such as mutual evaluations, reports or published follow-up reports, has not established effective AML/CFT systems that are in accordance with the recommendations of the Financial Action Task Force, or that is considered a low tax rate territory	Ask the Client to provide additional information about the purpose of establishing the Business Relationship and his/her economic activities. Gathering additional information and documents for the purpose of identifying the source and origin of the funds used in a transaction. Ask the Client to provide additional information about its links with the said country

14. REPORTING

14.1 If the relevant employee has a suspicion that he or she may be dealing with suspicious or unusual behaviour, the relevant employee shall promptly report this to the Compliance

Officer.

14.2 The relevant employee is not allowed to notify the customer about the fact that the customer has been reported to the Compliance Officer.

14.3 In case of any suspicion, the relevant employee must notify the Compliance Officer. The Compliance Officer must consider each report to determine whether it gives rise to grounds for knowledge or suspicion. Where such suspicion is determined, a suspicious transaction report made by the Compliance Officer shall be sent to the FMS.

14.4 In case of suspicion of terrorist financing, the relevant employee must identify the risk customer and report to the Compliance Officer if the risks belonging to a customer cannot be reasonably mitigated or explained.

15. COMPLIANCE OFFICER

15.1 The Compliance Officer shall have the following duties:

a. Checking compliance with the money laundering prevention requirements and carrying out training for the employees.
b. Carrying out preliminary analysis of submitted reports and deciding whether or not to refer a report to the FMS.
c. Sending information to the FMS in the case of suspected money laundering and responding to queries and precepts made by the FMS when applicable in accordance to Georgian law.

d. Gathering information received from employees about suspicious and/or unusual actions, processing such information and keeping records pursuant to the prescribed procedure.

15.2 The rights of the Compliance Officer:

a. Making proposals for amending these Rules, AML policy, and any other policies of our company that are related to anti-money laundering and the prevention of terrorist financing;
b. Monitoring the activities of the employees in pursuing the measures to prevent money laundering and terrorist financing.
c. Receiving data and information required for performance of the duties of the Compliance Officer.
d. Making proposals for re-organising the process of submission of notifications of suspicious and unusual transactions.
e. Receiving training in the field.

15.3 The Compliance Officer may send the information or data that have become known to him or her in connection with suspected money laundering only to:

f. The management board of the company or to an employee especially appointed by the management board.

g. The FMS.
h. The court on the basis of a court ruling or judgement.

16. REPORTING TO THE FMS

16.1 In the event of a well-founded suspicion concerning money laundering or terrorist financing, the Compliance Officer shall promptly report it to the FMS.

16.2 A report shall be sent to the FMS using the web-based reporting form at https://www.fms.gov.ge/eng/page/online-reporting-system. If a report is communicated orally, the Compliance Officer shall duplicate it in writing during the next day at the latest.

16.3 The customer shall never be notified about any report sent about him or her to the FMS.

16.4 If the activities of a customer are not, in accordance with these Rules, fully classifiable as activities which are to be reported to the FMS, any future activities of such customer shall be under increased scrutiny. The FMS shall be notified immediately if there is a well- founded suspicion about the behaviour of the customer.

16.5 Reporting to the FMS and sending relevant information shall not be deemed to be a violation of the duty of confidentiality laid down by law or a contract and no liability prescribed by legislation or a contract shall be attributed to those persons for disclosure of such relevant information.

17. INTERNAL CONTROL RULES OF THE RELEVANT EMPLOYEES

17.1 The Compliance Officer is responsible for checking the work done by the relevant employee.

17.2 The Compliance Officer shall check the work of the relevant employee in accordance with the following criteria:

a. the work of the relevant employee does not breach the Rules;
b. the relevant employee has done sufficient research on the customer;
c. the relevant employee has documented all the evidences about the customer;
d. the relevant employee has made a decision relying on the evidence collected and documented.

17.3 The relevant employee may get a low-quality notification from the Compliance Officer if the relevant employee constantly breaches the criteria. In case the quality of the

employee's work has not been improved after the first notification, this may lead to extraordinary termination.

18. TRAINING

18.1 The Compliance Officer or other expert in the field of anti-money laundering shall carry out the money laundering and terrorist financing prevention training for the employees of our company.

18.2 The Compliance Officer is responsible for carrying out regular training. Each employee shall confirm their participation with their signature. It is recommended to organize training when necessary.

18.3 The Compliance Officer is obligated to provide instructions and an introduction training to all new relevant employees pursuant to the prescribed procedure following the signing of the employment contract no later than within one week after the commencement of employment by the relevant employee and to make the new relevant employee familiar with these Rules against signature.

18.4 The Compliance Officer has the right to submit proposals concerning what training should be made to the management board.

19. REQUESTS FROM THE FMS

19.1. Upon the request of a supervision officer of the FMS all necessary documents and information shall be provided to the inspectors immediately.