KNOW YOUR CLIENT/ANTI-MONEY LAUNDERING POLICY

Last updated: April [•], 2018

1. PURPOSE OF THIS KNOW YOUR CLIENT/ANTI-MONEY LAUNDERING POLICY

1.1. In this know your client ("KYC")/anti-money laundering ("AML") policy ("Policy") we, [•], located at [•] ("Company"), create principles and procedures to identify Company's customers and prohibit and actively prevent money laundering and any activity that facilitate money laundering or the financing of terrorist or criminal activities. This Policy shall apply to any and all customers who wish to purchase Company's tokens (demand for Company's services to be provided to a token holder under terms and conditions of terms of token sale and other applicable documents located at Company's website https://nwpsolution.com ("Website")) during token sale regardless to any circumstances, including, but not limited to payment method (fiat currencies, crypto currencies) and/or any other terms and conditions; token sale procedure is governed by separate terms of token sale located at Website.

1.2. When it is required by the applicable laws and regulations, Company will has a designated compliance officer ("Officer"), who will have full responsibility for this Policy and applicable procedures. The duties of the Officer shall include, but not limited to, monitoring Company's compliance with this Policy, KYC/AML/CFT related obligations, overseeing communication and training for employees.

1.3. Company has implemented the following rules and procedures towards the purpose of this Policy:

(a) AML/KYC Compliance officer (Officer);
(b) risk-based management and risk assessment;
(c) customer due diligence, identification and identity verification (KYC);
(d) AML/CFT high risk countries and restricted countries;
(e) AML screening;
(f) ongoing monitoring of all transaction, suspicious transactions identification and reporting;
(g) training program;
(h) recordkeeping.

2. CUSTOMERS DUE DILIGENCE AND "KNOW YOUR CLIENT" IDENTIFICATION PROGRAM

2.1. Company will collect all information and documents from each customer of Company's Services who has opened an account to enable the customer to be identified under this Policy based on the following principles: (a) risk-based management to verify identity of each customer, (b) recording of all information and documents, verification methods and results, (c) providing customers with notice that Company will seek identification information to verity customers' identities, (d) comparing information and documents provided by a

customer, as well as customer's identity with government lists of suspected terrorists and/or sanctioned persons.

2.2. High risk countries and restricted countries. For each customer that meet one or several of the following criteria Company will enhance its customers due diligence program to evaluate risks, and to detect and report (when needed) suspicious activity: (a) legal person incorporation in offshore jurisdiction and/or customer's shareholder(s) is incorporated in offshore jurisdiction, (b) individual person from high risk and monitored jurisdictions (based on FATF publications in effect from time to time, OECD lists in effect from time to time, UN/EU/USA and other international and national sanctions lists when persons included in such lists may be provided with services by the Company), (c) information and/or documents provided by a client during customers due diligence of questionable origin (collectively, the "High Risk Countries"). In all such cases Company shall take all necessary and reasonable steps to enhance its customers due diligence requirements and procedures, that may include the following: (a) request of reference from a financial institution, (b) request for an evidence of source of funds, (c) any other requests and verification means that will help Company to form a reasonable belief that it knows the true identity of a customer and sources of his/her funds.

Company will refuse in selling and distribution of tokens or services to a customer who/which is (a) a permanent residence permit (green card) holder in the United States of America, or (b) a citizen or a resident (tax or otherwise) of the United States of America, Puerto Rico, the Virgin Islands of United States, or any other possessions of the United States of America, or People's Republic of China, South Korea or a person of these states or (c) a citizen or resident (tax or otherwise) of any country or territory where transactions with digital tokens and/or digital currencies are prohibited or in any other manner restricted by applicable law, (d) to a person included in the Watchlists Databases (as defined below). "Person" is generally defined as a natural person residing in the relevant state or any entity organized or incorporated under the laws of the relevant state. Purchased tokens cannot be offered or distributed as well as cannot be resold or otherwise alienated by their holders to mentioned persons.

2.3. Company has will maintain and procure the following risk-based Customer due diligence and KYC identification program workflow that may be amended by the Company from time to time:

(a) customers shall provide information and documents specified in section 2.3 to verify their identity. Based on risk assessment in case of high risk countries and/or other terms provided herein and/or to be implemented and/or ensured under applicable laws and regulations Company will request additional information and/or documents;

(b) all provided information and documents will be verified by the Company, Officer and KYC/AML service provider (Onfido Limited, located at 40 Long Acre, London WC2E 9LG, United Kingdom, and/or other KYC/AML service provider that may be engaged by the Company from time to time, collectively, the "KYC/AML Service

Provider") in compliance with applicable laws and regulations and this Policy, that will includes the following steps: (i) customer open an account, (ii) customer fill his/her account with information and documents provided in section 2.3, (iii) provided by a customer information will be transferred to the KYC/AML Service Provider in order to verify customer's identity, (iv) the KYC/AML Service Provider will verify provided information and documents and verify a customer or decline in a customer verification, the KYC/AML Service Provider will also perform research on the Government Sanctions Lists, Politically Exposed Persons Lists, Anti-Terrorism Watchlists, Anti-Money Laundering (AML) Watchlists, CIA Watchlists, Global Watchlist, Disqualified Directors (collectively the "Watchlists Databases"), (v) Company and/or KYC/AML Service Provider will verify customer's residence based on the information and documents provided by a customer under the section 2.3, (iv) should customer is an individual person or legal entity from the High Risk Countries, then Company will perform any additional reasonable steps based on risk-based approach or refuse such customer in provision of tokens and/or services and refund to that customer any funds that have been previously deposited by such customer to the account to the originated address (account) in the same type and manner within reasonable time, unless otherwise is provided in this Policy and/or required by the applicable laws and regulations;

(c) Company will from time to time request from customer additional information and/or documents to update KYC/AML, as well as in cases provided by applicable laws and regulations and/or herein.

2.4. Once customer open an account, Company will collect the following information and/or documents for all and any accounts, any person (individual person, entity, company, partnership, incorporation, organization, other form of legal entity/person ("legal person")) that is opening a new account and whose name is on the account prior to providing any tokens or services to such person, including receiving Company's services and/or goods (deposits of digital, crypto and/or fiat currencies and/or digital assets does not require prior customers due diligence):

(a) name;

(b) date of birth (for an individual person) or date of incorporation (for a legal person);

(c) nationality;

(d) gender;

(e) email;

(f) phone number;

(g) proof of identity (passport, driving license or government issued identity card that includes picture of a holder) for an individual person;

(h) proof of a residential address: electricity, gas, water or other similar utility bill less than three months old or a bank statement (for an individual person) or a registered address or other location (for a legal person);

(i) photograph (“selfie”, for an individual person) or certificate of incorporation, memorandum and articles of association, beneficial owners information and such legal person directors’ identity documents/information provided above and proof of a residential address (for a legal person).

Company may reasonably request any other information and/or documents needed to verify customers identity. Company may also from time to time requests any customer to update information and/or documents previously provided to the Company. In each case as reasonable requested by the Company, a customer shall provide a written evidence of the identity and source of funds (digital, virtual and/or fiat currencies and/or digital assets, collectively “funds”) he/she intended to use in order to receive Company’s services and/or goods. Such evidence may be provided via separate message or through any other means presented and/or used by the Company, including by incorporation of such evidence in public offer to be accepted prior to using of services/delivery of goods.

2.5. Based on the risk, that shall be determined on case by case basis, and to the extent reasonable, using risk-based procedures to verify and document all and any information received by the Company in regards to a customer, Company will ensure and make all necessary efforts to form a reasonable belief that Company (a) know the true identity of a customer and (b) information and documents provided by a customer are accurate and true. Company, Officer and KYC/AML Service Provider will analyze all and information and documents received and/or collected by the Company and/or Officer and/or KYC/AML Service Provider from a customer and/or any other reasonable sources, including, but not limited to, governmental websites, any other websites, databases, other public and available for the Company and/or Officer and/or KYC/AML Service Provider sources, information and/or documents, whether such information and/or documents are sufficient to form a reasonable belief that Company know the true identity of a customer. Customer’s identify may be verified through documentary and/or non-documentary (including, electronically) means. Company may use any of appropriate verify method based of each case risks.

When requested by the Company and/or KYC/AML Service Provider all documents to be provided by a customer shall be certified by a lawyer, accountant, notary public or official of customer’s nationality embassy or consulate. In such case certifier must state that a document is a true copy of the original one, and must sign and date each copy of the documents and indicate his/her position or capacity on such

documents and provide necessary contact details. This clause shall also apply to any non-English language documents that requires to be translated and certified.

Company may use any non-documentary means of customer identity verification available to the Company, including, but not limited to, confirming of customer's email, confirming of customer's phone number, arranging a video call with customer (through Skype, Zoom or any other available software), addressing a customer to the KYC/AML Service Provider.

Company will conduct procedures necessary for identity verification within reasonable time after the account is opened, but in all cases prior to providing services/delivery of goods by the Company to such unverified customers. Based on applicable risks and case by case basis, Company may refuse to complete any transaction, including, but not limited to, depositing of funds to customer's account, before Company verified the information and/or documents in regards to such transaction and/or customer.

Company shall has the right to engage any other appropriate service provider to verify customers identity and/or rely on its performance of some or all of the steps of Company's customers due diligence; should customer failed to be identified by such third person, Company shall take all actions prescribed by this Policy.

2.6. In event the Company and/or Officer and/or KYC/AML Service Provider find suspicious information in information and/or documents provided by a customer that indicated possible money laundering, terrorist financing activity or any other suspicious activity, Company and/or Officer will report the activity in accordance with applicable laws and regulations.

2.7. Company recognize the risk that customer's name and true identity may be hidden by certain means, including, but not limited to, acting in the name of legal person or trust that may be created or conducted business and operational activities in a jurisdiction that has been designated as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. Hence, Company may create and maintain different levels of clearance in regards to groups of customers based on allowed deposits amount and services to be provided to such customers and shall in each case notify customer on required information and/or documents to be provided. Company also may take all necessary and reasonable steps to verify a customer or an individual and/or legal persons associated and/or connected with a customer when standard methods used by Company reasonable to be insufficient.

2.8. When Company cannot form a reasonable belief that it know the true identity of a customer (or in regards to a legal person – its beneficial owners and/or directors), Company shall do the following: (a) deactivate customer's account and keep it in deactivated status until, (b) close such an account after multiple attempts to verify customer's identity fail, (c) refund to that customer any funds that have been

previously deposited by such customer to the account to the originated address (account) in the same type and manner within reasonable time, unless otherwise is provided in this Policy and/or required by the applicable laws and regulations, and (d) determine whether it is necessary to notify authorities when such notification is required by the applicable laws and regulations.

2.9. In a potential or actual customer either refuses to provide any part of the information described above when requested by the Company or Company reasonably believe and/or have found that customer have intentionally provided false, wrong and/or misleading information, then Company will deactivate such customer account and consider closing any existing account. Any funds that have been previously deposited by such customer shall be refunded to that customer to the originated address (account) in the same type and manner within reasonable time, unless otherwise is provided in this Policy and/or required by the applicable laws and regulations. Company and Officer will notify authorities in all cases when such notifications are required by the applicable laws and regulations.

2.10. In all cases Company, will provide a notice to customers that Company will request information from them to verify their identities as it required by applicable laws and regulations. Company will inform customers by email or through Company's software when a customer wants to receive Company's services and/or goods, or, then it is reasonably decided by the Company – prior to depositing of any funds. Company shall also has the right to publish messages in customer's account designated for each user.

3. ONGOING MONITORING, SUSPICIOUS ACTIVITY AND SUSPICIOUS TRANSACTIONS REPORTING

3.1. Company and/or Officer will monitor any customer account activity for unusual size, volume, pattern or type of operations, transactions, communications or actions taking into account risk factors and flags that are appropriate to Company's business on risk based approach. Red flags that signal possible money laundering and/or terrorist financing include, but not limited to:

(a) insufficient, suspicious information/documents or information/documents of questionable origin (provided documents cannot be verified etc.);
(b) certain funds transfer activities (many small, incoming transfers or deposits, transfers or deposits from offshores etc.);
(c) activity inconsistent with business (maintaining multiple accounts in the name of other individual persons etc.).

In each and every case, Company and/or Officer will decide whether or not and how to further investigate such suspicious activity.

3.2. Company will report or notify authorities when such notification or report is required by the applicable laws and regulations. In each case, including suspicious activity, Company may fill a voluntary report.

3.3. Company will keep and maintain all and any information and documents in regards to AML/CFT procedures. All such information and documents are highly confidential and will not be provided by the Company to any third party, unless otherwise is specified herein or prescribed by applicable laws and regulations.

4. TRAINING PROGRAMS

4.1. Company will develop and maintain ongoing employee training, which will include, but not limited to: (a) how to identify red flags and signs of money laundering and/or financing of terrorism that arise during the course of the employees' duties, (b) what to do once the risk is identified, (c) Company's KYC policy and procedures, (d) Company's recordkeeping politics and duties, (e) disciplinary, civil and criminal consequences of non-compliance with KYC/AML/CFT applicable laws and regulations.

5. RECORDKEEPING

5.1. Company will keep and maintain all and any logs of verifications, including all and any identifying information provided by a customer and third parties as described herein, and all steps and resolutions made by the Company within the verification process. Company will keep and maintain records containing the following:

(a) in respect to documentary verification - all and any information and documents that Company relied on to verify a customer's identity;

(b) in respect to non-documentary verification – all and any information and logs that describe the methods and the results of any steps that Company took to verify the identity of a customer.

(c) in respect to verification based on third party verifying services provider – information of customer's verification status and logs/messages between Company and such third party in regards to such customer.

All and any information to be kept in regards to customers verifications are highly confidential and will not be provided by the Company to any third party, unless otherwise is specified herein or prescribed by applicable laws and regulations. Information and/or document by the KYC/AML Service Provider may be provided to authorities through an additional request.