ANTI MONEY LAUNDERING POLICY (EU)

PW HOLDINGS CORP.

PW Holdings Corp., hereinafter referred to as the "Company," which term shall refer to and include its owners, its subsidiaries and affiliated companies, directors, investors, employees, officers, representatives, affiliates, or other related parties.

WHEREAS, Persons availing of the any services from the Company or engaging in any transactions on any digital/non-digital platform provided or operated by Company directly or indirectly, are referred to herein, as "Users".

WHEREAS, This is an agreement between the Company and the User, which is binding on the User. All Users are required to comply with the terms of this agreement at all times, and any instance of non-compliance will result in the termination of such user's accounts on the Company platform, and in appropriate reporting of the circumstances of such non-compliance and such termination to the relevant statutory authorities.

WHEREAS, Integrity, honesty and ethical business practices are some of the core values of the Company, and the Company strongly condemns any and all activities related to terrorism, money laundering, and all other unlawful actions. In order to prevent misuse of the services provided on the Company's platform, Users are required to strictly comply with the terms contained herein, which forms part and parcel of the User Terms of Service. Terms not defined herein shall carry the same meaning as in the Terms & Conditions, and in the absence thereof, to general usage and parlance.

WHEREAS, Users are required to read, review, understand and then agree to the terms hereunder for using or availing of the Company's platform. If user do not agree with any terms herein, then user should not register with the Company's platform

WHEREAS, This Anti-Money Laundering Policy (hereinafter referred to as the "AML Policy") supersedes and replaces any and all prior oral or written understandings or agreements between the Company and the User with respect to the AML Policy.

Introduction

Money laundering is criminalized primarily by means of the Law 656 which has adopted an "all crimes" approach. Law 656 also establishes the The National Office for Prevention and Control of Money Laundering ("NOPCML"). Law 656 further implements the provisions of Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing and of Directive 2006/70/EC of the European Commission of 1 August 2006 laying down implementing measures.

The regulations contain detailed provisions on the measures and procedures to be maintained and applied by subject persons, including customer due diligence measures, record keeping procedures and reporting procedures, and identify the subject persons to such measures and

procedures are applicable launderer and reintroduced into the economy e.g. by the purchase of a legitimate asset.

Law 656 is supplemented by the Implementing Procedures issued by the NOPCML.The Implementing Procedures provide an interpretation of the regulations and their purpose is to guide and assist subject persons in understanding and fulfilling their obligations under the regulations, thus ensuring effective implementation thereof. The Implementing Procedures are binding on subject persons and failure to comply is subject to an administrative penalty.

1. Definitions

All terms defined in the Terms of Service and the Privacy Policy will carry the same meaning, force and effect in this AML Policy.

1.1 "Applicable Law" means all laws in force for the time being within the territory of Romania, including (but not restricted to) Law 656 (the "Controlling Law")

1.2 "Designated Director" means a managing director or whole-time director of the Company who has been appointed and authorized to administer the Company's anti-money laundering measures, in accordance with the Controlling Law;

1.3 'NOPCML' refers to the Unit responsible for ensuring that the Controlling Law and ancillary legislation are implemented into our laws. It is a government agency having a distinct legal personality which is responsible for the implementation of the AML regime in Romania, for monitoring compliance with the relevant legislative provisions, and for the collection, collation, processing, analysis and dissemination of information with a view to combating ML and Funding of Terrorism.

1.4 Money-Laundering "ML" refers to:

(i) the conversion or transfer of property knowing or suspecting that such property is derived directly or indirectly from, or the proceeds of, criminal activity or from an act or acts of participation in criminal activity, for or purposes of concealing or disguising the origin of the property or of assisting any person or persons involved or concerned in criminal activity;

(ii) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect of, in or over, or ownership of property, knowing or suspecting that such property is derived directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

(iii) the acquisition, possession or use of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

(iv) retention without reasonable excuse of property knowing or suspecting that the same was derived or originated directly or indirectly from criminal activity or from an act or acts of participation in criminal activity;

(v) attempting any of the matters or activities defined in the above foregoing sub-paragraphs (i), (ii), (iii) and(vi) within the meaning of the Controlling Law

This definition is rather an exhaustive list of acts that would be considered as ML under Romanian law. In fact, passive possession of criminal property is also considered to amount to the offence of ML.

1.5 “PEP” refers to natural persons who are or have been entrusted with prominent public functions, their immediate family members or persons known to be close associates of such persons but shall not include middle ranking or more junior officials.

(i) the term ‘natural persons who are or have been entrusted with prominent public functions’ shall include:

(a) Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;

(b) Members of Parliament;

(c) Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;

(d) Members of courts, Audit Committees or of the boards of central banks;

(e) Ambassadors and other high-ranking officers in the armed forces;

(f) Members of the administration, management or boards of State-owned corporations,

And where applicable, for the purposes of sub-paragraphs (a) to (e), shall include positions held at the Community or international level;

(ii) the term ‘immediate family members’ shall include the following:

(a) the spouse, or any partner recognized by national law as equivalent to the spouse;

(b) the children and their spouses or partners; and

(c) the parents;

(iii) the term ‘persons known to be close associates’ shall include the following:

(a) a natural person known to have joint beneficial ownership of a body corporate or any other form of legal arrangement, or any other close business relations with that PEP;

(b) a natural person who has sole beneficial ownership of a body corporate or any other form of legal arrangement that is known to have been established for the benefit of that PEP.

1.6 “Principal Officer” means the officer appointed by the Company to administer the company’s anti-money laundering measures, in accordance with the Controlling Law;

1.7 “Senior Management” means such directors, officers or other personnel of the Company as are specifically designated to monitor and ensure know-your-customer compliance and the operation of the Company’s internal audit systems;

1.8 “Suspicious Transaction” means a transaction, whether or not made in cash which, to a person acting in good faith:

(i) give rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified in the Controlling Law, regardless of the value involved; or

(ii) appears to be made in circumstances of unusual or unjustified complexity; or

(iii) appears to have no economic rationale or bona fide purpose; or

(iv) gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism;

Explanation —Transaction involving financing of the activities relating to terrorism includes transaction involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

2. The MLRO

2.1 A local AMLO (Anti Money Laundering Officer) has been appointed who directly reports to the local management and for whom the local management is directly responsible.The local AMLO is committed to undertake the following tasks:

(i) Receive internal reports of suspicious transactions;

(ii) Endeavour to ensure the Company has a fully integrated Chain Analysis tool for all Crypto-wallets and to monitor all incoming and outgoing transactions.

(iii) Review the Know-Your- Client (KYC) process from the NOPCML website. In completing this report MLROs should provide as much detail as possible together with the relevant identification and other supporting documentation. To ensure the highest level of confidentiality subject-persons should submit the STR using the FIAU’s online portal and should refrain from making any disclosures by email;

(iv) Any manual submission of the STR should be delivered by hand to the NOPCML premises addressed to the Director at the hereunder address. In such cases the template downloaded from the NOPCML website shall be signed by the MLRO;

(v) In cases of urgency an initial disclosure may be made by telephone on the number provided below, but a written report shall then be submitted within the shortest time possible, either through the NOPCML's online portal or by hand;

(vi) It should be noted that STRs should only be filed with the NOPCML and should not be copied to any supervisory authority;

(vii) Make external reporting to the relevant local authorities wherever applicable;

(viii) Provide annual reporting to the local management (the report should cover the results of any AML control activities, notification of suspicious transactions, employee training, implemented AML prevention activities);

(ix) Examine all unusual and conspicuous transactions and behaviour either as an outcome from monitoring systems or otherwise detected;

(x) Daily check of Users against recognized "black lists" (e.g. OFAC), aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable;

(xi) Develop procedures and policies to detect and prevent money laundering;

(xii) Periodically review the effectiveness of policies and procedures with regards to prevention and reporting of any illegal activity;

(xiii) Establish staff training; and

(xiv) Advise and inform all employees

2.2. The Board of Directors of the service provider shall appoint an individual as the MLRO. The person chosen shall be an officer of the service provider and a person who is of sufficient seniority and command. In other words, when choosing a person for the post of MLRO, the Board of Directors of the service provider shall ensure that such person is an individual who is employed by the service provider and, thus, such responsibility, according to the IPs, cannot be outsourced to third parties.

2.3 Moreover, the person appointed to the post of MLRO is to have a certain standing within the service provider and thus cannot be a non-executive director. S/he is to be chosen from among those persons having a certain seniority.

2.4 The MLRO shall be responsible for overseeing all aspects of the service provider's AML/ CFT activities. The service provider shall ensure that the MLRO has sufficient resources available to him or her in order to ensure compliance with the Service Provider's AML/ CFT policy.The MLRO shall be responsible for:

(i) receiving reports of knowledge or suspicion of ML/ Funding of Terrorism;

(ii) considering such reports to determine whether knowledge or suspicion of ML/Funding of Terrorism subsists;

(iii) reporting knowledge or suspicion of ML/ Funding of Terrorism to the NOPCML; and

(iv) responding promptly to any request for information made by the NOPCML.

2.5 Once the MLRO is appointed, the service provider shall submit a detailed fact sheet to the NOPCML in the same form as is available on the NOPCML website. This form, or any amendment thereof, may be downloaded from the NOPCML's website and submitted online. The NOPCML shall be notified of any changes thereafter.

2.6 Should the MLRO resign and a new individual is appointed instead, the NOPCML shall be notified within fifteen (15) days from the resignation thereof and the previous MLRO shall provide the NOPCML with an explanation as to why s/he decided to resign.

3. Maintenance of Records

3.1 The Company shall maintain a record of, and has evolved an internal mechanism to detect, the following:

(i) Details pertaining to User transactions, including but not limited to:

(a) the nature of the transactions;

(b) the amount of the transaction and the currency in which it was denominated;

(c) the date on which the transaction was conducted; and

(d) the parties to the transaction.

(ii) All details for the following categories of User transactions, separately from those recorded under (i) above:

(a) User transactions of value of at least EUR 2,500 (Two Thousand and Five Hundred Euros), or its foreign currency equivalent;

(b) and User transactions that are connected to each other and that take place within a month of each other, with a monthly aggregate of at least EUR 2,500 (Two Thousand and Five Hundred Euros), or its foreign currency equivalent; and

(iii) All Suspicious Transactions by way of deposits and credits, withdrawals into or from any accounts in whatsoever name they are referred to in any currency maintained by way of cheques including third party cheques, pay orders, demand drafts, or any other instrument of payment of money including electronic receipts or credits and electronic payments or debits; or

transfers from one account within the same banking company, financial institution and intermediary, or any other mode in whatsoever name it is referred to;

(iv) credits or debits into or from any non-monetary accounts in any currency maintained by the Company;

(v) money transfer or remittances in favor of own Users or non-Users from Romania or abroad and to third party beneficiaries in Romania or abroad including transactions on its own account in any currency by any of the following:

(a) demand drafts, or

(b) telegraphic or wire transfers or electronic remittances or transfers, or

(c) internet transfers, or

(d) Automated Clearing House remittances, or

(e) any other mode of money transfer by whatsoever name called;

4. Procedure and Manner of Maintaining Information

4.1 The Company will maintain hard and soft copies of the above-mentioned records of Transactions in accordance with the procedure and manner, as may be specified under applicable laws or regulations, from time to time.

4.2 In addition to the above, the Company shall maintain records of transactions, as per its prevailing processes.

5. Disclosure of Records:

5.1 The Company may be required and / or directed to cooperate and aid the government and / or law enforcement authorities, police, investigating agencies, or Tribunals and Courts within the territory of Romania or from outside the said territory.

5.2 In such cases, subject to applicable laws with respect to data protection, the Company shall be entitled to disclose any information about the User that is in its possession or control, including to government or law enforcement officials, police, investigating agencies, Tribunals and Courts within the territory of Romania.

5.3 In particular, the Company shall be entitled to initiate processes and disclosures, including but not limited to the following circumstances:

(i) information pertaining to or in pursuance of claims and legal process (such as summons / warrants);

(ii) to protect the Company’s property, rights, and safety and the property, rights, and safety of a third party or the public in general;

(iii) to identify and stop any activity that the Company considers illegal, unethical, or legally actionable.

5.4 The Company may, if so required under applicable Law, disclose the following information to NOPCML, as appointed under the Controlling Law:

(i) Name, designation and address of the Designated Director, the Principal Officer and all Senior Management;

(ii) User transactions listed in II(a)(ii) above by the 15th day of each succeeding month, or more frequently if so instructed by the authorities;

(iii) User transactions listed in II(a)(iii) within seven working days of being satisfied that the transaction in question is suspicious in nature, or more frequently if so instructed by the authorities.

5.5 The Company also compiles records and audit and compliance notes to determine the efficacy of its internal audit systems on an ongoing basis, and such notes are submitted to the Company's audit committee on a quarterly basis for this purpose.

6. Client Risk Categorization

6.1 Based on the various factors and risk parameters, the clients shall be categorized into High, medium and low risk category.

6.2 Certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction, etc. The illustrative factors for risk profiling is given as under (list is indicative and can be expanded as per business requirements and experience):

(i) Geographical Location and Category of client.

(ii) Nature of Business activity

(iii) Financial Health vs Trade Volume

(iv) Income Range

6.3 Risk based Monitoring approach shall be followed. Broad categories of monitoring and reason for suspicion and examples of suspicious transactions for the Company are indicated as under:

(i) Identity of Client

(a) False identification documents

(b) Identification documents which could not be verified within reasonable time.

(c) Doubt over the real beneficiary of the account.

(d) Accounts opened with names very close to other established business entities

(ii) Suspicious Background

(a) Suspicious background or links with known criminals

(iii) Multiple Accounts

(a) Large number of accounts having a common account holder or authorized signatory with no rationale.

(b) Unexplained transfers between multiple accounts with no rationale

(iv) Activity in Accounts

(a) Unusual activity compared to past transactions

(b) Sudden activity in dormant accounts

(c) Activity inconsistent with what would be expected from declared business

(v) Nature of Transactions

(a) Unusual or unjustified complexity

(b) No economic rationale or bonafide purpose

(c) Source of funds/Cryptocurrencies are doubtful

(vi) Value of Transactions

(a)Value just under the reporting threshold amount in an apparent attempt to avoid reporting

(b) Inconsistent with the clients apparent financial standing

(c) Inconsistency in the transactions pattern by Customers.

6.4The Company will ensure that information sought from the customer is relevant to the perceived risk, is not intrusive, and is in conformity with the guidelines issued in this regard. Any other information from the customer will be sought separately with the client's consent and after opening the account.

7. Exception Handling

Exceptions to this Policy must be approved by the Chief Compliance Officer, or a designated person. All exceptions must be documented, with reasons for the exceptions, including expiration or review date and, wherever necessary, include an action plan and timelines for compliance with the policy.No accounts will be opened by the Company for any User who appears on the United Nations Security Council's ISIL (Da'esh) & Al-Qaida Sanctions List, or on its 1988 Sanctions List.

8. EDD [Enhanced Due-Diligence]

8.1 In risk-sensitive instances or where the customer is not present e.g. due to online applications via its platform, the service provider shall apply EDD measures. EDD measures are additional measures to the CDD measures.

8.2 EDD measures are applied in order to ensure that the higher risks presented by certain Customers and transactions are better monitored and managed to avoid any involvement in ML/Funding of Terrorism.Thus, the service provider applies EDD measures when the Operations Department classifies the Customer as high risk and, in all cases, where the customer is not present.

8.3 EDD measures are applied in the following cases:

(i) where the Applicant has not been physically present for identification purposes subject to the service provider's CDD measures;

(ii) in relation to cross-border correspondent banking relationships; or

(iii) in relation to a Business Relationship or Occasional Transaction with a PEP.

8.4 In the above-mentioned instances, the MLRO and the Designated Employee/s are to be consulted in order to confirm which of the EDD measures indicated hereunder are to be applied whenever the applicant is not present (i.e. for non-face-to-face applicants i.e. online applications).

8.5 In addition to the three (3) specific instances mentioned above, the service provider shall also conduct EDD measures in relation to a Business Relationship or a transaction connected to a jurisdiction listed under the public documents issued by the FATF as required in the guidance note on high-risk and non-cooperative jurisdictions and reported on the NOPCML's website

8.6 The Controlling Law requires the service provider as an SP to inform the NOPCML of any Business Relationships or transactions with persons, companies and undertakings, including those carrying out relevant financial business or a relevant activity from a non-Reputable Jurisdiction which continues not to apply measures equivalent to those laid down in Applicable Legislation.Therefore, when any of the service provider's representative/s working closely with Customers notes the above, they are to report such matters to the MLRO. The MLRO shall thereafter follow the procedure indicated in the Reporting Section.

8.7 Although only three (3) relationships are mentioned above, there may be other situations which, by their nature, can present a higher risk of ML/ Funding of Terrorism. The MLRO shall, therefore, use his discretion when applying EDD measures in such situations. The MLRO shall ensure that such measures are applied on a risk-sensitive basis and should be appropriate in view of the higher risk of ML/ Funding of Terrorism.

NON-FACE-TO-FACE APPLICANTS

In addition to the identification and verification of identity measures to be carried out in accordance with the Identification and Verification of the Customer Section, the Operations Department shall apply one (1) or more of the following measures:

A) ENSURE THAT THE FIRST PAYMENT OR TRANSACTION INTO THE ACCOUNT IS CARRIED OUT THROUGH AN ACCOUNT HELD BY THE APPLICANT IN THER NAME WITH A CREDIT INSTITUTION AUTHORISED UNDER THE LAWS OF ROMANIA OR OTHERWISE AUTHORISED IN ANOTHER MEMBER STATE OF THE COMMUNITY OR IN A REPUTABLE JURISDICTION.

This measure entails a bank-to-bank transfer from an existing account through which the Customer would have already been identified by the service provider. Therefore, the first payment or transaction into the account held by the Applicant may be an electronic card payment only where the electronic card used to affect the payment is linked to an account held by the payer with a credit institution. In such instance, the Customer must provide the service provider's statement form the same Bank that prove that the credit card used is liked to Customer's account with that Bank. Pre-paid credit cards and E-money payments are not admissible for EDD purposes.

POLITICALLY EXPOSED-PERSONS (PEPs)

At the initial on-boarding stage (or if the client has been flagged as a PEP from a new review): The service provider shall obtain such information directly from the Applicant (as part of the on-boarding questions) or from other readily available sources such as Experian, World Check, newspapers etc (the service provider will automatically check if the Applicant is flagged as a PEP in the Watchlists of Experian on an automated basis). The Board of Directors' approval is required in those cases where the Customer is categorized as a PEP. The application of EDD measures to PEPs is mandatory as long as the PEP remains entrusted with a prominent public function for a subsequent twelve (12) months from when he ceases to be so entrusted.

9. Ongoing Due Diligence Measures For Transactions On The Company's Platform

9.1 The Company shall exercise ongoing due diligence with respect to the business relationship with every User and closely examine the transactions in order to ensure that they are consistent with their knowledge of the User, his business and risk profile and where necessary, the source of funds.

9.2 The Company will also review its due diligence measures and undertake measures to re-verify the identity of a User and obtain further information on a User's activities, if the Company has any suspicions of money laundering or the financing of terrorism.

9.3 All due diligence undertaken by the Company is documented, designed to consider all relevant risk factors in determining overall risk and the appropriate mitigation measures, is kept up to date; and will always be available to the relevant authorities and self-regulating bodies.

9.4 The Company will verify the identity of Users while carrying out transactions worth at least EUR 2,500 (Two Thousand and Five Hundred Euros), whether through a single transaction or a series of connected transactions. If the Company has reason to believe that a User is intentionally structuring a transaction into a series of transactions, below the threshold thereof.

9.5 Once a User has participated in transactions of a total value of at least over the course of his/her engagement with the Company platform, or deposits or transacts in an amount of at least EUR 2,500 (Two Thousand and Five Hundred Euros) on the Company's Platform, the Company will also conduct 'chain analysis' to identify the relevant public address for such User and earmark such User as either as 'high risk', 'medium risk', or 'low risk' based on parameters such as the use of cryptocurrencies by such Users at online gambling websites, darknet websites, etc.This limit EUR 2,500 (Two Thousand and Five Hundred Euros)may be revised by the Company from time to time, based on the Company's determination of appropriate thresholds in accordance with ongoing compliance measures, and if so required under applicable Law.

9.6 The Company will, in particular, monitor the following categories of transactions, and will conduct due diligence on an ongoing basis on them:

(i) large, complex transactions, including those with unusual patterns that are inconsistent with a User's normal / expected level of activity, without an apparent economic rationale or legitimate purpose; and

(ii) transactions that involve high account turnover, inconsistent with the size of the balance ordinarily maintained by a User.

9.7 As Users are not face-to-face customers of The Company, The Company may required to undertake enhanced due diligence, including certification of all documents provided by the Users, calling for additional documents whenever necessary, and requiring that the first payments made by such Users be effected through the User's KYC-compliant account with a bank. Any such requirements, as may be imposed under Applicable Law, will be incorporated into this AML Policy, and The Company reserves the right to update the AML Policy for this purpose.

9.8 The Company's staff are trained in The Company's due diligence and anti-money laundering measures, as well as all requirements prescribed under Applicable Law for this purpose and may be contacted if any User has questions or concerns about any of measures contained in this AML Policy.

10. SUSPICIOUS TRANSACTION REPORT (STR)

10.1 In the event of knowledge or suspicion of ML/ Funding of Terrorism, and any knowledge, suspicion or reasonable grounds to suspect that the funds used in a transaction are the proceeds of a crime, the service provider shall proceed as follows:

(i) the service provider's employee who has knowledge or suspicion of such ML/ Funding of Terrorism, shall report this matter to the MLRO.

(ii) once the MLRO has received all information relating to the knowledge or suspicion reported by the employee, he shall, together with the assistance of the Designated Employee/s, carry out a further investigation into the matter in order to decide whether such report is to be submitted to the NOPCML as an STR.

(iii) if the MLRO decides not to submit the report, he shall prepare a detailed report explaining his findings and the reasons for his decision and such report shall be kept in the service provider's records and retained for a period of five (5) years in accordance with the Record Keeping Section above.

(iv) if on the other hand, the MLRO decides to submit the report to the NOPCML, he shall complete the report in the form prescribed by the NOPCML. This form may be filed online through the NOPCML website indicated above.

10.2 Any disclosures to the NOPCML are to be made as soon as practicable, but in no circumstance, later than five (5) working days from when the knowledge or suspicion of ML/ Funding of Terrorism arises or from the existence of reasonable grounds to suspect ML/ Funding of Terrorism.

10.3 The five (5) working daysshall be considered to start to run in accordance with the provisions of the following paragraphs:

(i) in cases where, subsequent to the receipt of an internal report, the MLRO determines, on the basis of the information contained in the report, or on the basis of additional information and, or documentation, that there is knowledge or suspicion of ML/ Funding of Terrorism, the five (5) working day period shall start to run from when such a determination is made by the MLRO;

(ii) notwithstanding the provisions of paragraph (a) above, where the service provider is in possession of information that constitutes a reasonable ground to suspect ML/ Funding of Terrorism, the five (5) working day period shall start to run from when the service provider came into possession of or became aware of that information.

11. Obligation On The Part Of The User

The User hereby agrees and undertakes to not indulge, assist, abet and encourage in any manner whatsoever, in any activity involving money laundering or financing of any illegal or unlawful activities.

12. Retention Of Records

The Company shall maintain such records of the identity of Users in and soft copies in a manner, as may be specified under applicable laws or regulations, from time to time, and in the absence thereof, from the date of cessation of the transactions between the User and The Company for a period ofTen years for ordinary transactions; andTwelve years in case of Suspicious Transactions

13. Notices

13.1 Any notice or other communication provided for in this Agreement shall be sent only through electronic mail. User hereby agrees to receive electronic or any other form of communication and notifications from The Company. Email messages sent over the Internet are not always secure and The Company is not responsible or liable for non-receipt of such communication by User. Once the email is dispatched by The Company, it shall be deemed to have been served on the User. The Company shall be deemed to have received communications from the User only upon actual receipt into the Inbox of the account of the person to whom such communication is addressed and acknowledged. The Company shall not be liable or responsible for non-receipt of communications or for any damages incurred by the result of sending email messages over the Internet.

13.2 All communications to User shall be at the electronic mail address provided by User, as part of the KYC norms. User shall ensure that any change in the electronic mail address or communication option is duly intimated to The Company.

14. Governing Law & Jurisdiction

14.1 This Agreement shall be governed by and construed in accordance with the laws of Romania.

14.2 The parties agree to irrevocably submit to the exclusive jurisdiction of the courts in Romania for the resolution of any disputes arising from this Agreement or in connection therewith or pursuant thereto.

15. Successors

This Agreement shall bind and inure to the benefit of the parties, and their respective successors and permitted assigns.

16. Severability

16.1 The invalidity or unenforceability of any provision of this Agreement shall not in any way affect, impair or render unenforceable this Agreement or any other provision contained herein, which shall remain in full force and effect.

16.2 This Agreement shall be considered divisible as to such provision, which is deemed to be invalid or unenforceable and the remainder of this Agreement shall be enforceable and binding on the Parties.

17. Waiver

No provision of this Agreement may be waived or changed except by a writing signed by the party against whom such waiver is sought to be enforced. The failure or omission by either party at any time to enforce or require strict or timely compliance to any provision of this Agreement shall not affect or impair that provision or any other provision in any way or the rights of such

party hereof, to avail itself of the remedies it may have in respect of any subsequent breach of that or any other provision.

18. Recitals

The Recitals, Schedules and Annexures in this Agreement shall form part of this Agreement and the contents thereof shall be read into this Agreement. Headings are for the purpose of easy reference and shall not affect the meaning or interpretation of this Agreement.

19. Entirety

This Agreement, and the other agreements contemplated hereby, constitute the entire agreement.

20. Government Approvals

21.1 This Agreement is subject to confirmation by the Government of Romania of the legality of facilitating the dealing in Cryptocurrencies (including bitcoins), and in the event that the Government of Romania was to hold that transactions involving cryptocurrencies are invalid or illegal in Romania, this Agreement shall stand automatically terminated without further notice to User.

22.2 The Company has given full disclosure to the current Government in relation to the Company's business and regulatory status and has sought discussions with the Government with respect to Cryptocurrencies including bitcoins in Romania and the risk involved in dealing with or investing in the same.The current regulatory status and permissibility of the use of cryptocurrencies, including bitcoins, in Romania is unclear. The User is deemed to have understood, agreed to and accepted the risk and costs of such investment.

21. Designated Director and Principal

The Company shall appoint a Principal Officer and a Designated Director and will designated Senior Management as required under Applicable Law, along with setting up a compliance team, who shall be responsible for ensuring compliance, monitoring transactions, and sharing and reporting information as required under the law/regulations.

22. Modifications

22.1 These terms may be periodically reviewed and revised. The revised terms will be uploaded on the Company's Website and will reflect the modified date of the terms. The User is required to periodically visit the website and review terms and any changes thereto.

22.2 Continued use of the Company's Services constitutes the agreement of User to the terms contained herein and any amendments thereto.

22.3 This agreement or the responsibilities or benefits arising therefrom cannot be assigned by User save and except with the prior written consent of the Company

23. Miscellaneous

All other provisions of the Company's Terms of Service shall be read into this policy and shall form part hereof, including Governing Laws and Jurisdiction, notices, severability, assignment and such or other provisions.

Updated: June, 2019