Anti-money laundering (AML) Policy

1. GENERAL PROVISIONS

1.1. This AML Policy, or rules of procedure for prevention of money laundering and terrorist financing, and compliance with international sanctions (hereinafter Rules) has been developed by Sincere Systems Group LTD, registration number 12695421 (hereinafter referred to as Company), in order to prevent entering into deals involving suspected Money Laundering and Terrorist Financing and to ensure identification and reporting of such. Any questions related to this policy should be addressed to:

Sincere Systems Group LTD or by e-mail to support@s-group.io.

1.2. The obligation to observe the Rules rests with Management Board members and employees of the Company, including temporary staff, agents of the Company who initiate or establish Business Relationship (as defined in section 2.6) (hereinafter all together called the Representative). Every Representative must confirm awareness of the Rules with the signature.

1.3. The Rules are primarily based on the regulations of Money Laundering and Terrorist Financing Prevention Act (hereinafter the Act) and International Sanctions Act (hereinafter ISA).

2. DEFINITIONS

2.1. Money Laundering — is a set of activities with the property derived from criminal activity or property obtained instead of such property with the purpose to:

I. conceal or disguise the true nature, source, location, disposition, movement, right of ownership or other rights related to such property; II. convert, transfer, acquire, possess or use such property for the purpose of concealing or disguising the illicit origin of property or of assisting a person who is involved in criminal activity to evade the legal consequences of his or her action;

III. participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in subsections 2.1.I and 2.1.II.

2.2. Terrorist Financing — acts of financing of terrorism as defined in § $237_3$of the Penal Code of Great Britain.

2.3. International Sanctions — list of non-military measures decided by the European Union, the United Nations, another international organization or the government of Great Britain and aimed to maintain or restore peace,

prevent conflicts and restore international security, support and reinforce democracy, follow the rule of law, human rights and international law and achieve other objectives of the common foreign and security policy of the European Union.

2.4. Compliance Officer or CO — representative appointed by the Management Board responsible for the effectiveness of the Rules, conducting compliance over the adherence to the Rules and serving as contact person of the FIU.

2.5. FIU — Financial Intelligence Unit of the Police and Border Guard Board of Great Britain.

2.6. Business Relationship — a relationship of the Company established in its economic and professional activities with the Client.

2.7. Client (User) — a natural or legal person, who uses services of the

Company. 2.8. Beneficial Owner — is a natural person, who:

I. Taking advantage of his influence, exercises control over a transaction, operation or another person and in whose interests or favour or on whose account a transaction or operation is performed taking advantage of his influence, makes a transaction, act, action, operation or step or otherwise exercises control over a transaction, act, action, operation or step or over another person and in whose interests or favour or on whose account a transaction or act, action, operation or step is made.

II. Ultimately owns or controls a legal person through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that person, including through bearer shareholdings, or through control via other means. Direct ownership is a manner of exercising control whereby a natural person holds a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company. Indirect ownership is a manner of exercising control whereby a company which is under the control of a natural person holds or multiple companies which are under the control of the same natural person hold a shareholding of 25 per cent plus one share or an ownership interest of more than 25 per cent in a company.

III. Holds the position of a senior managing official, if, after all possible means of identification have been exhausted, the person specified in clause ii cannot be identified and there is no doubt that such person exists or where there are doubts as to whether the identified person is a beneficial owner.

IV. In the case of a trust, civil law partnership, community or legal

arrangement, the beneficial owner is the natural person who ultimately controls the association via direct or indirect ownership or otherwise and is such

associations': settlor or person who has handed over property to the asset pool, trustee or manager or possessor of the property, person ensuring and controlling the preservation of property, where such person has been appointed, or the beneficiary, or where the beneficiary or beneficiaries have yet to be determined, the class of persons in whose main interest such association is set up or operates.

2.9. Politically Exposed Person or PEP — is a natural person who is or who has been entrusted with prominent public functions including a head of state, head of government, minister and deputy or assistant minister; 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; an ambassador, a chargé d'affaires and a high-ranking officer in the armed forces; a member of an administrative, management or supervisory body of a state-owned enterprise; a director, deputy director and member of the board or equivalent function of an international organisation, except middle ranking or more junior officials.

2.9.1. The provisions set out above also include positions in the European Union and in other international organizations.

2.9.2. A family member of a person performing prominent public functions is the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a child and their spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; a parent of a politically exposed person.

2.9.3. A close associate of a person performing prominent public functions is 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; and 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.

2.10. Local Politically Exposed Person or local PEP — a natural person, who performs or has performed prominent public functions in Great Britain, a contracting state of the European Economic Area or in an institution of European Union.

2.11. Company — Sincere Systems Group LTD, registration number 12695421.

2.12. Management Board or MB — management board of the Company. Member of the MB, as appointed by relevant MB decision, is responsible for implementation of the Rules.

3. AML COMPLIANCE OFFICER

3.1. The Company appointed a Compliance Officer ("CO"), who is fully responsible for the execution of the Rules and reports to the MB any material breaches of the internal AML policy and procedures and of the regulations, codes, and standards of good practice.

3.2. AML Compliance Officer's responsibilities include:

I. request appropriate identity documents to identify the Client and its representatives;

II. request documents and information regarding the activities of the Client and legal origin of funds;

III. request information about Beneficial Owners of a legal person;

IV. screen the risk profile of the Client, select the appropriate CDD measures, assess the

V. risk whether the Client is or may become involved in Money Laundering or Terrorist

VI. Financing;

VII. re-identify the Client or the representative of the Client, if there are any doubts regarding the correctness of the information received in the course of initial identification.

If the Client is a natural person, the following data shall be recorded: Full name of the Client;

3.2.1. monitor the compliance of the Rules with the relevant laws and compliance of the activity of the Representatives with the procedures established by the Rules;

3.2.2. compile and keep updated the data regarding countries with low tax risk, high and low risk of Money Laundering and Terrorist Financing and economical activities with great exposure to Money Laundering and Terrorist Financing;

3.2.3. carry out training, instruct and update the Representatives on matters pertaining to procedures for prevention of Money Laundering and Terrorist Financing;

3.2.4. report to the MB once a year (or more frequently, if necessary) on compliance with the Rules, and on circumstances with a suspicion of Money Laundering or Terrorist Financing;

3.2.5. collect, process and analyze the data received from the Representatives or Clients concerning suspicious and unusual activities;

3.2.6. collaborate with and report to the FIU on events of suspected Money Laundering or Terrorist Financing, and respond to inquiries of the FIU;

3.2.7. make proposals on remedying any deficiencies identified in the course of checks.

4. CLIENT IDENTIFICATION

4.1. Company follows one of the main international standards for the prevention of illegal activities, namely CDD — Customer Due Diligence (“CDD”). CDD measures include the following procedures:

I. Identifying the Client and verifying its identity using reliable, independent sources, documents or data, including e-identifying; II. Identifying and verifying of the representative of the Client and the right of representation;

III. Identifying the Client's Beneficial Owner;

IV. Conducting ongoing CDD on the Client's business to ensure the Company’s knowledge of the Client and its source of funds is correct;

V. Obtaining information whether the Client is a PEP or PEP’s family member or PEP’s close associate.

4.2. To comply with the DD obligation, the Representatives have the right to request:

4.3.

I. Information regarding identification and verification of the right of representation. If the right of representation does not arise from law, the name of the document used for establishing and verification of the right of representation, the date of issue, and the name or name of the issuing party;

II. Email address;

III.Phone number and Telegram messenger contact;

IV. IV. Occupation.

4.4. If the Client is a legal person, the following data shall be recorded:

I. Name of the Client;

II. Registry code (or registration number and registration date) of the

Client;

III. Names and authorizations of members of the Management Board or the head of branch or the other relevant body;

IV. Telecommunications numbers;

V. Email address;

VI. Phone number.

4.5. Having received identification information, employees of the Company have the right to verify its authenticity by requesting relevant documents from the Client.

4.6. In case of Clients being natural persons and the representatives of Clients, the following documents can be used for identification:

I. Personal ID card (whether ID card, e-resident card or residence permit card);

II. Passport or diplomatic passport;

III. Travel document issued in a foreign country;

IV. Driving licence (if it has name, facial image, signature and personal code or date of birth of holder on it).

4.7. In case of Clients being legal persons, their legal capacity shall be identified and verified on the basis of the following documents:

I. in case of legal persons registered in Great Britain and branches of foreign companies registered in Great Britain, the identification shall be conducted on the basis of an extract of a registry card of commercial register;

II. foreign legal persons shall be identified on the basis of an extract of the relevant register or a transcript of the registration certificate or an equal document, which has been issued by competent authority or body not earlier that six months before submission there of;

III. personal identification code (in case of absence the date and place of birth and place of residence);

IV. articles and memorandum of association;

V. documents confirming the management and ownership structure.

4.8. Where applicable, the representative of a Client shall submit a document in the required format certifying the right of representation.

4.9. Relevant documents to verify the address of the Client include, but are not limited to, the following:

I. a copy of the utility bill (landline telephone, water, electricity) not older then 3 months at the place of registration of the Client;

II. a copy of the tax or tariff bill from the local government;
III. copy of bank statement (for current account, deposit account or credit card).

4.10. If the Company has reason to believe that a business relationship with the Client represents a high risk, the Company is entitled to request the following information from the Client:

I. information relating to the source of the Client's funds or wealth; II. additional information necessary for clarification of this issue from the Client.

4.11. If not, original documents are used for identification, the Representative shall control and verify data by using at least two reliable and independent sources.

4.12. The Company is entitled to receive information about the Client from additional sources, from third parties, if the Company has reason to believe that business relations with the Client represent a high risk.

4.13. When receiving information to verify information from the Client about the source of funds, including virtual currency assets or wealth, the Company's employees will request and analyze details of the status, employment or business/profession of the Client.

4.14. Company employees have the right to request additional data or evidence of this employment / occupation, which may be deemed necessary in a situation, in particular, relevant supporting documents (labor agreements, bank statements, letters from the employer or the Client's company, etc.).

4.15. If the Company doubts the correctness of the data, documents provided by the Client or reveals his suspicious activity, the Company asks the Client to undergo additional verification, which includes high definition photos of the Client with a paper where indicated date and inscription "Sincere Systems Group LTD".

4.16. To use payment bank cards at the Company websitehttps://sincere.systems (the Website), the Client may be asked by the Company to undergo a special verification procedure in accordance with AML requirements.

4.17. The Company has the right to freeze the account of any Client in the event that he / she is suspected / in suspicious activity that may be related to money laundering. If the Client, being a citizen of the USA, registered on the Website under false documents and data, his account will be deleted without returning of funds.

4.18. After the final confirmation of the Client identity Company has the right to refuse the potential legal liability for those situations when its services will be used for criminal activities.

4.19. According to the existing standards of practical activities to resist money laundering, Company reserves the right to require the Client additional documents or any other additional information necessary for identification of the natural or legal person, or verify the transaction performed by the Client **5.**

MONEY LAUNDERING MONITORING

5.1. The Company has the right to conduct ongoing checks of the Clients. In particular, it concerns the regular review and updating of the Company's information on what its Clients do, the level of risk they pose if something contradicts the information or beliefs received earlier from the Client.

5.2. The Company's AML monitoring program will make periodic assessments of the adequacy of its systems and controls arrangements to prevent the Company being used to further financial crime. The CO reports these findings to MB and governing body on a periodic and at least annual basis.

5.3. In accordance with the law requirements and security reasons, Company might provide limited services on account opening and carrying transaction processing for citizens and residents of, as well as people staying in the countries where transactions are prohibited by international sanctions.

5.4. Company implements the above-mentioned International Sanctions to the extent determined by the UN, the EU, the U.S., or state bodies (i.e., the Government). Therefore, Company will not engage in any actions that directly or indirectly evade the Financial Sanctions. For accurate understanding, Company does not work with Users from countries and regions ("Restricted Countries"):

- Afghanistan;
- Albania;
- Barbados;
- Belarus;
- Botswana;
- Burkina Faso
- Cambodia;
- Cayman Islands;
- Crimea, Sevastopol;
- Cuba;
- Democratic People's Republic of Korea (DPRK);
- Donetsk, Luhansk regions of Ukraine;
- Ghana;
- Haiti;
- Iran;
- Iraq;
- Jamaica;
- Jordan;
- Mali;
- Mainland China;
- Mauritius;
- Morocco;
- Myanmar;
- Nicaragua;
- Ontario (Canada);
- Pakistan;
- Panama;
- Philippines;
- Quebec (Canada);
- Russian Federation;
- Senegal;
- Singapore;

- Somalia;
- South Sudan
- Sudan;
- Syria;
- The Bahamas •
Transnistria region; •
Trinidad and Tobago;
- Turkey;
- Uganda;
- United States; •
Vanuatu;
- Venezuela;
- Yemen;
- Zimbabwe.

These geographic restrictions are applied according to lists defined by the relevant authorities and might be subject to updates from time to time.