Powerchain.Energy OU KYC/AML/CFT POLICY

1. Introduction

1.1. This document is drafted in accordance and in compliance with rules and regulations imposed in terms of the Estonian Money Laundering and Terrorist Financing Prevention Act ("**the Act**") as it relates to providers defined in Section 2 (1) 10 & 11 of the Act:-

"*(1) This Act applies to the economic and professional activities of the following persons*

… 10) providers of a service exchanging a virtual currency against a fiat currency;

11) providers of a virtual currency wallet service"

1.2. In terms of the Act providers, who are obliged entities, are legally required to take commensurate steps to prevent any activities which would constitute criminal activity such as money laundering or the financing of terrorist acts, when conducting business with its customers.

1.3. In meeting this requirements of the Act, procedures and policies must be documented for:-

1.3.1. suitably identifying the all parties who engage in any transactions with the company, through a due diligence as contemplated in Section 20 of the Act;

1.3.2. criteria for risk assessments and list of risk activities;

1.3.3. instructions where the company has a suspicion of money laundering and terrorist financing or an unusual transaction or circumstance involved; and

1.3.4. instructions for effectively identifying whether a person is a politically exposed person ("**PEP**") or a local PEP subject to international sanctions or a person whose place of residence or seat is in a high risk third country or country which meets the requirements of subsection 4 of Section 37 of the Act; and

1.3.5. appointing a management board member in charge of implementing the Act and compliance officer.

2. Customer Due Diligence ("CDD")

Requirements for natural persons

2.1. In terms of Section 19(1) of the Act, the company is obliged to apply the following due diligence measure upon the establishment of a business relationship by obtaining from customers who are natural persons in their personal capacity:-

2.1.1. the name of the natural person:

2.1.2. the national identity document and personal identification code (in the case of local customers) and foreign passports or other valid travel document (in the case of foreign customers);

2.1.3. the document conferring the right of representation, if not on a legal basis, with the name of the party conferring the right of representation;

2.1.4. proof of registration with the tax authority in the jurisdiction in which the customer has its head office, and where it is an Estonian natural person then proof of registration with the Tax and Customs Board must be furnished;

2.1.5. proof of operating address (utility bill, rental agreement with affidavit from landlord etc.)

Requirements for legal persons and corporations

2.2. In terms of section 22 of the Act, a legal person registered in Estonia, the branch of a foreign company registered in Estonia and a foreign legal person, shall furnish the company with the following details:-

2.2.1. The name or business name of the legal person;

2.2.2. registry code or registration number and date of registration;

2.2.3. names of the directors, members of the management board or other body replacing the management board and their authorisation in representing the legal person;

2.2.4. the national identity document and personal identification code (in the case of local customers) and foreign passports or other valid travel document (in the case of foreign customers) of all directors and shareholders (holding 25% plus 1 of the total shares in the company);

2.2.5. the telecommunication and other contact details;

2.2.6. registry card and/or registration certificate; and

2.2.7. representative of a legal person of a foreign country must, at the request of the company, submit a document certifying his powers authenticated by a notary or in accordance with an equal procedure and legalised or certified be a certificate replacing legislation (apostille);

2.2.8. proof of registration with the tax authority in the jurisdiction in which the customer has its head office, and where it is an Estonian company, or a foreign company having a registered subsidiary or affiliated company in Estonia then proof of registration with the Tax and Customs Board must be furnished;

2.2.9. proof of operating address (utility bill, rental agreement with affidavit from landlord etc.)

2.3. Upon receipt of the information as envisaged in this paragraph 2 and any time thereafter, the company may screen the risk profile of the customer to assess the risk of whether the customer may become involved in money laundering or terrorist financing, in accordance with the risk assessment matrix made reference to at paragraph 3 below.

2.4. The company, its representatives, authorised agents, directors, shareholders, employees or any other similar party shall under no circumstances:-

2.4.1.give an order not to implement money laundering and terrorist financing due diligence measures, risk assessment, procedural rules and internal control rules;

2.4.2. open an anonymous account or savings book;

2.4.3. fail to verify the identity of customers as envisaged in this paragraph 2;

2.4.4. conclude a transaction with a politically exposed person as defined at Section 3(11) of the Act, the characteristics of which are set out paragraph 6 below;

2.4.5. outsource any activity to a person established in a high risk country, as made reference to at paragraph 3.2. below;

2.4.6. fail to report any suspicious transactional activity to the Financial Intelligence Unit; and

2.4.7. fail to register and retain data as contemplated in the Act.

3. Risk Assessment and Categories

3.1. The company shall assess risks associated with its customers according to an assessment to be conducted in accordance with the following table, and will adjust the CDD accordingly:

RISK	NORMAL	HIGHER	THE HIGHEST
WHEN	The risk level is normal, there are no high risk characteristics	1. The place of residence of employment of business of a customer is in a country which is included in the list of risk countries 2. The customer is a local PEP or a person associated with a PEP 3. The legal person is registered in the European Economic Area or in Switzerland, whose area of activity is associated with enhanced money laundering risk 4. The legal person is situated in a country which is listed in the list of risk countries 5. The legal person is a non-profit association, trust, civil law	1. The customer is suspected to be or to have been linked with a financial offence or other suspicious activities. 2. The customer is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries 3. There is information that legal person is suspected to be or to have been linked with a financial offence or other suspicious activities 4. There is information that legal person is suspected to be or to have been linked with a financial offence or other

		partnership or another contractual legal arrangement, whose activities and liability are insufficiently regulated by law, and the legality of financing of which is not easy to screen. 6. The representative or the Beneficial Owner / Shareholder of a legal person is a local PEP or his / her family member.	suspicious activities. 5. legal person registered outside the European Economic Area, whose field of business is associated with a high risk of Money Laundering, or registered in a low tax rate country, as made reference to at paragraph 3.2 below
DUE DILIGENCE REQUIREMENTS	**SIMPLIFIED DUE DILIGENCE (SECTION 8 OF THE ACT) AS MADE REFERENCE TO AT PARAGRAPH 2 ABOVE**	**NORMAL DUE DILIGENCE (SECTION 6 OF THE ACT) AS MADE REFERENCE TO AT PARAGRAPH 2 ABOVE**	**ENHANCED DUE DILIGENCE (SECTION 9 OF THE ACT) AS MADE REFERENCE TO AT PARAGRAPH 2 ABOVE**
	- a company listed on a regulated market that is subject to disclosure requirements consistent with European Union law; - a legal person governed by public law	- upon establishing a new business relationship; - in the event of insufficiency or suspected incorrectness of the documents or information gathered previously in the	The risk level of the customer is higher The customer is a person associated with a PEP - The customer is PEP or local PEP; - The actual place of residence or

	founded in Estonia; - a governmental authority or another authority performing public functions in Estonia or a contracting state of the European Economic Area; - an authority of the European Union; - a credit institution or a financial institution, acting on behalf of itself, located in a contracting state of the European Economic Area or in a third country which in the country of location is subject to equal requirements and the performance of which is subject to state supervision	course of carrying out CDD measures made reference to at paragraph 2 above; - upon suspicion of money laundering or terrorist financing	employment or business of a customer is in a country, which is included in the list of risk countries - the customer is suspected to be or to have been linked with a financial offence or other suspicious activities - customer is a non-resident individual, whose place of residence or activities is in a country, which is listed in the list of risk countries - when suspicion arises regarding truthfulness of the provided data and/or of authenticity of the identification documents regarding the customer or its Beneficial Owners - in a situation with higher risk of money laundering and terrorists financing - in case of companies that

			have nominee shareholders or shares in bearer form
MEASURES	**Include in addition to the CDD made reference to at paragraph 2 above**	**Include in addition to the CDD made reference to at paragraph 2 above**	**In addition to the CDD made reference to at paragraph 2 above**
	– the customer can be identified on the basis of publicly available information; – the ownership and control structure of the customer is transparent and constant; – the operations of the customer and their accounting or payment policies are transparent; – customer reports to and is controlled by an authority of executive power of Estonia or a contracting state of the European Economic Area, another agency performing public duties, or an authority of the European Union.	– Identification of a natural person (Identification details and copy of ID documents), video call in case of deposit of more than 15.000 EUR – Identification of a legal person (Corporate details, Certificate of incorporation, Articles of association, ID of representatives and shareholders)	– the customer can be identified on the basis of publicly available information; – the ownership and control structure of the customer is transparent and constant; – the operations of the customer and their accounting or payment policies are transparent; – Identification and verification of a customer on the basis of additional documents, data or information, which originates from a reliable and independent source – Identification and verification of a customer while being present at the same place

			– Asking the identification or verification documents to be notarised or officially authenticated – Obtaining additional information on the purpose and nature of the Business Relationship and verification from a reliable and independent source – Reassessment of a risk profile of a customer not later than 6 months after establishment of Business Relationship

3.2. For the purposes of the Act risk countries are distinguished as follows:-

3.2.1. countries which according to the Financial Action Task Force do not follow the requirements for prevention of money laundering and terrorism financing including, Democratic People's Republic of China, Ethiopia, Iran, Pakistan, Serbia, Sri Lanka, Syria, Trinidad and Tobago, Tunisia and Yemen;

3.2.2. countries which according to the Financial Intelligence Unit pose a significant terrorist threat, which includes Afghanistan, Algeria, United Arab Emirates, Bahrein, Bangladesh, Egypt, Indonesia, Iraq, Iran, Yemen, Jordanian, Qatar, Kuwait, Lebanon, Libya, Malaysia, Mali, Morocco, Mauritania, Nigeria, Oman, Pakistan, Palestine, Saudi Arabia, Somalia, Sri Lanka, Sudan, Syria, Tunisia, Turkey, Ethnic groups of Caucasus belonging to Russian Federation (Chechens, Lesgid, ossetians, Ingushes etc.)

3.3. The company shall update their process for risk assessment and analysis from time to time, but, it shall implement same through data analysis, suspicion

detection tools and by performing a variety of compliance related tasks such as data capturing, filtering, record keeping, investigation management and reporting.

3.4. Some of the system functionalities may include:-

3.4.1. daily check of customers against recognized “black lists” (eg OFAC);

3.4.2. aggregating transfers by multiple data points;

3.4.3. placing customers on watch and service denial lists;

3.4.4. opening cases for investigation where needed; and

3.4.5. sending internal communications and filling out statutory reports, if applicable.

4. Reporting Procedure to the Financial Intelligence Unit

4.1. The company has a duty to report any activity whose characteristics refer to the use of criminal proceeds, terrorist financing or related **offences within 2 working days** from identify such activity to the Financial Intelligence Unit, in terms of Section 49 of the Act.

4.2. Where an employee, auditor, duly authorised agent, director, member of the management board, or related person identifies a suspicious activity as contemplated at paragraph 4.1. above, the compliance officer must be notified, with all supporting documentation.

4.3. The compliance officer, must assess the report, and should the report be correct then the compliance officer may submit same.

4.4. The company must further notify the Financial Intelligence Unit of any transaction where there is a pecuniary obligation of over 32,000 Euros, or its equivalent in another currency, within one year.

4.5. The company must submit all supporting documentation in relation to the transaction or activity, including documentation compiled in terms of paragraph 2 hereof to the Financial Intelligence Unit, via its online form or X-road service.

4.6. All reports made in terms of this paragraph 4 shall remain confidential and no information of the party who reports the suspicious activity to the compliance officer shall be made public.

4.7. The Financial Intelligence Unit may be contacted at Police and Border Guard Board, Toostuse 52, 10416, Talinn, Telephone (+372) 612 3840, Facsimile (+372) 612 3845, e-mail: rahapesu@politisei.ee

5. Identifying Criteria of PEPs

5.1. In terms of Section 3 (11) of the Act a politically exposed person is:-

5.1.1. a natural person entrusted with prominent public functions;

5.1.2. public functions include 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

5.1.3. As part of the KYC questionnaire each public official must review each of the above functions and ensure that they provide full particulars concerning their role and function.

5.1.4. Middle ranking and junior officials are exempt from PEP classification.

5.1.5. If the party is identified as a PEP or foreign PEP the risk assessment and due diligence must be conducted at the highest level as contemplated at paragraph 3 of this policy.

6. Compliance Officer

6.1. The company shall appoint one management board member to act as the party responsible for overseeing and implementing the provisions of the Act and this policy, if the company has more than 2 (two) management board members.

6.2. Within 5 (five) working days of the appointment of the management board member as contemplated at paragraph 6.1. the member may appoint a compliance officer, who shall act solely or as the head of a team which shall implement compliance protocols in accordance with the Act.

6.3. The compliance officer shall immediately advise the Financial Intelligence Unit and any other party of their appointment.

6.4. The compliance officer shall be required to perform the following duties:-

6.4.1. organisation of the collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of

money laundering or terrorist financing, which have become evident in the activities of the obliged entity;

6.4.2. reporting to the Financial Intelligence Unit in the event of suspicion of money laundering or terrorist financing;

6.4.3. periodic submission of written statements on compliance with the requirements arising from the Act to the management board of a credit institution or financial institution or to the director of the branch of a foreign credit institution or financial institution registered in the Estonian commercial register;

6.4.5. performance of other duties and obligations related to compliance with the requirements of the Act.

6.5. A compliance officer has the right to:-

6.5.1. make proposals to the management board of a credit or financial institution or to the director of the branch of a foreign credit or financial institution registered in the Estonian commercial register for amendment and modification of the rules of procedure containing AML/CFT requirements and organisation of training specified in subsection 6 of section 14 of the Act;

6.5.2. demand that a structural unit of the obliged entity eliminate within a reasonable time deficiencies identified in the implementation of the AML/CFT requirements;

6.5.3. receive data and information required for performance of the duties of a compliance officer;

6.5.4. make proposals for organisation of the process of submission of notifications of suspicious and unusual transactions;

6.5.5. receive training in the field.