Last Updated: August 3, 2018

Version: 1.00

Deneum KYC and AML Policy

1. AML/KYC POLICY STATUS AND ACCEPTANCE

1.1. This AML/KYC Policy (hereinafter referred to as the "Policy") sets forth the general rules and procedures governing the implementation and conduction of Know-Your-Customer ("KYC") procedures in accordance with the relevant Anti-Money Laundering rules ("AML").

1.2. Each User must carefully read and comply with this Policy. It is understood and presumed per se that by the fact of the Website use and DNM Tokens purchase during the Deneum Token Sale or otherwise, the respective User fully read, understood and accepted this Policy. If any User does not agree with this Policy in general or any part of it, such User must not access and use the Website and/or purchase DNM Tokens.

1.3. By agreeing to this Policy You acknowledge and agree that We maintain verification levels that require User participation and verification to obtain, with levelled permissions based on user-supplied information, Our ability to verify it, and Our internal policies. You accept that You may not be able to achieve Your desired level of verification, and We reserve the right, at Our sole discretion, to determine the appropriate verification level for any User, as well as the right to downgrade Users without notice. We may, from time to time, implement policies restricting verification levels by nationality, country of residence, or any other factor. This may affect Your right to purchase DNM Tokens or withdraw DNM Tokens in your Account, and You indemnify Us against any losses associated with an inability to purchase, withdraw, or use DNM Tokens based on Your verification level.

1.4. The Company reserves the right to modify or amend this Policy at its sole discretion. Any revisions to this AML/KYC Policy will be posted on the homepage of our Website. If we make changes, we will notify you by revising the date at the top of this Policy. We strongly recommend You to periodically visit the Website to review any changes that may be made to this AML/KYC Policy to stay updated on our AML/KYC practices. Your continued usage of the Website and/or services shall mean Your acceptance of those amendments.

1.5. In terms of the Deneum Token Sale this Policy shall be considered as inalienable part of the Deneum Token Sale Agreement, Deneum Privacy Policy and Terms of Use. In terms not regulated by this Policy, the Deneum Token Sale Agreement shall apply to the relationships that arise hereunder.

1.6. This Policy is administered by Company's Board of Directors (the "Board")

1.7. It is the personal obligation and responsibility of each Employee to act in a manner consistent with this Policy.

1.8. All Employees must report any breaches, violations, risks, incidents and complaints, as appropriate.

2. DEFINITIONS

2.1. **Applicable Law** – laws of Estonia are applicable under this Policy to any and all relations between a User and Company.

2.2. **Employee** – a Deneum employee.

2.3. **Personal Information** - information or totality of information that can be associated with a specific person (the User) and can be used to identify that person. The rules governing the Personal Information collection, processing and use by Deneum are documented in a separate Privacy Policy, which can be accessed via this link: www.deneum.com/privacy-policy.pdf.

2.4. **AML/KYC Policy** (also referred to as **"Policy**") – this AML/KYC Policy posted on the homepage of our Website which may be revised or updated from time to time as stated in subsection 1.4 of this AML/KYC Policy.

2.5. **Company**, **We**, **Us** – Deneum OU - a company incorporated under the legislation of Estonia for the purpose of Deneum project development and implementation, not being a financial entity, stock, exchange, investment entity or a partner, employer, agent or adviser for any User OR a third party, which we hire to perform services on our behalf such as Identity Verification Provider.

2.6. **Deneum** (also referred to as "**Platform**") is a blockchain-based platform for Token Sale and promotion of the technology based on innovative methods of transforming heat into electricity to reach the highest possible efficiency The technology is grounded on the interaction between atoms of deuterium inside titanium when heated under specific conditions.

2.7. **Deneum Token Sale** ("**Token Sale**", "**Crowdsale**") – an offering of DNM Tokens to eligible Users to purchase DNM Tokens during the Sale Period, according to the respective phases (launches) and DNM Tokens Price described on the Website and in Whitepaper.

2.8. **DNM Tokens** ("**DNM**", "**Tokens**") – cryptographic tokens, which are software digital products (not being cryptocurrency), which are created by the Company and is a digital representation for participation in Deneum project, including the participation in distribution of Platform rewards.

2.9. **Identity Verification Provider –** companies and/or services involved by Deneum OU for provision of KYC/ AML check such as www.icosid.com and/or www.sumsub.com.

2.10. **User** (also referred to as "**You**") – any person, who uses the Website, with or without prior registration and authorization using the account and purchases DNM Tokens. The Company reserves its right to set forth at any time upon its own discretion special eligibility or other requirements to certain Users to participate in a certain phase of Deneum Token Sale as shall be mentioned on the Website and Whitepaper.

2.11. **Website** – the website maintained and owned by the Company at www.deneum.com

2.12. **Whitepaper** – one of the official accompanying documents published by the Company on the Website, describing technical and marketing details of the Deneum Token Sale, the idea and purpose of the Deneum Platform, as well as DNM Tokens Price and Tokens Sale Period.

3. AML/KYC POLICY

3.1. Company is strongly committed to preventing the use of its operations for money laundering or any activity which facilitates money laundering, or the funding of terrorist or criminal activities.

3.2. On a global level, in order to prevent and combat money laundering and terrorism financing, there has been an introduction of the number of laws concerning the customer identification and verification procedures including but not limited to the EU AMLD5 Directive, which brings the virtual currencies under the scope of the Anti-Money Laundering Directive.

3.3. In the United States regulation of the AML is carried out by a special government body under the US Treasury – FinCEN. In particular, FinCEN regulates, so-called, "money services business" (MSB). In 2013 FinCEN published the clarification on the regulation of persons administering, exchanging or using virtual currencies bringing the businesses dealing with virtual currencies under the scope of AML/KYC in terms of spotting suspicious financial behavior.

3.4. In order to ensure that our operations are compliant with the AML/KYC rules and procedures, we are implementing the AML/KYC policies detailed below.

3.5. As part of our AML (Anti-Money Laundering) Policy in order to combat money laundering and illegal financing activities the Company follows the customer risk assessment principles that include but are not limited to the following:

– raise awareness on money laundering issues;

– assist law agencies and authorities to trace, seize, and confiscate the proceed of criminal activities;

– freeze any funds deemed suspicious and investigate the source of finance;

– introduce a Know-Your-Customer Policy (KYC);

– exercise reasonable measures to obtain information about the true identity of the persons on whose behalf a transaction is made;

– record keeping procedures – maintain, for a specific time period, all necessary records on transactions, both domestic and international;

– pay special attention to all complex, unusually large transactions;

– adopt economic, administrative, self-regulatory and other measures which can be taken to create an effective shield against money laundering;

– train staff accordingly;

– employ proper care in the hiring of new staff.

3.6. As part of the customer risk assessment, the following will act as Money Laundering Warning Signs based on guidance provided by Financial Action Task Force (FATF) – international body set up to combat money laundering:

– customer tells that the funds are coming from one source but then at the last minute the source changes;

– evasiveness or reluctance to provide information;

– incomplete or inconsistent information;

– unusual money transfer or transactions (e.g. when customer deposits unusual amounts (e.g. 9,990 euros) so as not to come under the threshold when KYC applies);

– complex group structures without obvious explanation that may be designed to disguise the true source and ownership of money;

– when money is coming from the list of 'high-risk and non-co-operative jurisdictions' according to FATF which can be accessed via this link: http://www.fatf-gafi.org/countries/#high-risk;

– negative public information available about the client or company.

3.7. The above principles and warning signs are aimed at determining the customer's risk in terms of propensity to commit money laundering, terrorist financing or identity theft.

3.8. Every Employee is required to act in furtherance of this policy statement to protect the Company from exploitation by money launderers or terrorists.

3.9. Company adopts the KYC (Know-Your-Customer) Policy and reserves the right to undertake KYC in order to verify the identity of its Users at any point.

3.10. As part of the exercise of this right, upon Company' request, User will immediately provide to Company all information of any type and documents that Company, in its sole discretion, deems necessary or appropriate to comply with any laws, regulations, rules or agreements, including without limitation judicial process. Such documents include but are not limited to:

- copy of passport or national ID (passport, driver's license; government identification cards)
- photographs of associated individuals;
- recent utility bill;

  'Recent' means no longer than 3 months from date of issue.

3.11. We also collect and process information Users provide directly to Company or to Identity Verification Provider when Users use our Services. Types of personal information which Company will collect from Users when Users visit or use our online services include your name, nationality, country of residence, postal address, personal or social security number, passport or other ID data (gender, date of birth, marital status, place of birth, passport or ID document number, photo, issue date, expiry date), telephone number(s), e-mail address, username or similar identifier and other.

Please note that the list above is not exhaustive and we reserve the right to require additional information at any time to verify the client's identification and to fully satisfy the latest Anti-Money Laundering rules.

3.12. We aim to reasonably identify each prospective User of DNM Tokens by cross-checking User data against governmental watch lists, including, but not limited to, the Specifically Designated Nationals and Blocked Persons List maintained by OFAC, Global Sanctions, PEP, Blacklist and Prohibited Countries and other watch lists.

3.13. We are also collaborating with various Identity Verification Providers that conduct on our behalf:

- Document Integrity Check including verification of the authenticity of photos and scanned copies of physical check documents;
- Identity Check including verification of a person's identity by matching User's passport data against data from multiple databases; and
- Face Match Check including confirmation of matches of an image of a person's face among a range of other photo images found in various documents, for example a passport, on name badge, a driver's license or other photo ID as well as selfies or avatar images.

3.14. If Your proposed purchase is flagged through Our internal controls, We may require additional proof of identification from You, and We have the right to not permit any Users until additional and verifiable proof of identity to our satisfaction is received and You have been approved as a prospective User.

3.15. The Personal Information requested as part of the KYC procedure will be collected, processed, used and stored in accordance with the General Data Protection Regulation (GDPR), rules and principles of which have been reflected in the Deneum Privacy Policy and implemented on the legal, technical and organizational level.

3.16. If any of the above documents are requested, prior to sending them to us we may require them to be certified as a true copy of the original by a Solicitor or a Lawyer who must use their company stamp. We require the documents to be sent to us in high quality color format. We reserve the right to reject any documents, which do not comply with the above or if we have doubts as to their veracity.

3.17. If any doubt arises we reserve the right to check the information provided, as part of the KYC Policy, using non-documentary methods including but not limited to contacting the customer directly.

3.18. Basing on results of KYC/AML checks we have a right to freeze any funds already transferred should the suspicion as to the sources of those funds arises after they have been deposited and investigate the customer's transaction in retrospect.

4. CONTACT DETAILS

4.1. If you have any questions regarding this AML/KYC Policy, please contact us at hello@deneum.com.