



AML/KYC POLICY

Anti-money Laundering and Know Your Customer Policy

The purpose of the EXENIUM Anti-Money Laundering and Know Your Customer Policy (hereinafter - the "AML/KYC Policy") is to identify, prevent and mitigate possible risks of EXENIUM being involved in illegal activity.

In conformity with international and local regulations EXENIUM has implemented effective internal procedures to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to react correspondingly in case of any form of suspicious activity from its Users.

AML/KYC Policy includes Verification procedures, Compliance Officer, Monitoring Transactions, Risk Assessment.

Customer due diligence ("CDD") has become one of one of the international standards for preventing illegal activity. Thus, EXENIUM has implemented its own verification procedures within the rigorous standards of anti-money laundering and "Know Your Customer" procedures.

The EXENIUM identification procedure requires the User to provide EXENIUM with reliable, independent source documents, data or information (for example, a national ID card, an international passport, an extract from the bank, a utility bill). For such purposes, EXENIUM reserves the right to collect the User's identification information for the purposes of AML / KYC Policy compliance.

EXENIUM will take steps to confirm the authenticity of documents and information provided by Users. All legal methods for double verification of identification information will be used, and EXENIUM reserves the right to investigate the cases of certain Users whose identities have been identified as dangerous or suspicious.

EXENIUM reserves the right to verify the identity of the User on an ongoing basis, especially when its identification information has been changed or its activities appear suspicious (unusual

for a particular User). In addition, EXENIUM reserves the right to request from the Users current documents, even if they have been authenticated in the past.

Information about the user's identification will be collected, stored, shared and protected strictly in accordance with the EXENIUM Privacy Policy and relevant rules.

After confirming the identity of the user, EXENIUM may refuse potential legal liability in a situation where the company's services are used to conduct illegal activities.

Users who intend to use payment cards for the purpose of consuming services must undergo a card check in accordance with the instructions available on the EXENIUM website.

The Compliance Officer is the person, duly authorized by EXENIUM, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of EXENIUM's anti-money laundering and counter-terrorist financing, in particular collecting Users' identification information, establishing and updating internal policies and procedures for the completion, review, submission and retention of all reports and records required under the applicable laws and regulations, monitoring transactions and investigating any significant deviations from normal activity, implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs, updating risk assessment regularly, providing law enforcement with information as required under the applicable laws and regulations.

The Compliance Officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activity.

The Users are known not only by verifying their identity by analyzing their transactional patterns. Therefore, EXENIUM relies on data analysis as a risk-assessment and suspicion detection tool. EXENIUM performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting. System functionalities include:

- 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;
- Case and document management.

In connection with the AML/KYC Policy, EXENIUM will monitor all transactions and it reserves the right to ensure that transactions of suspicious nature are reported to the proper law enforcement through the Compliance Officer; request the User to provide any additional information and documents in case of suspicious transactions; suspend or terminate User's Account when EXENIUM has suspicion that such User engaged in illegal activity.

However, the above list is not exhaustive and the Compliance Officer will monitor Users' transactions on a regular basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as *bona fide*.

EXENIUM, in line with the international requirements, has adopted a risk-based approach to combating money laundering and terrorist financing. By adopting a risk-based approach, EXENIUM is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks.