AML/KYC Policy

Introduction Gecobit OÜ Anti-Money Laundering and Know Your Customer Policy (hereinafter - the “AML/KYC Policy”) is designated to prevent and mitigate possible risks of Gecobit OÜ being involved in any kind of illegal activity. Both international and local regulations require Gecobit OÜ to implement effective internal procedures and mechanisms to prevent money laundering, terrorist financing, drug and human trafficking, proliferation of weapons of mass destruction, corruption and bribery and to take action in case of any form of suspicious activity from its customers. These requirements are created to prevent Gecobit OÜ , our employees, partners and clients from being misused for money laundering, terrorist financing or any other financial crime, by doing the following;

• Performing an enterprise-wide risk assessment to determine the risk profile of the Company.
• Establishing AML policies and procedures.
• Implementing internal controls throughout its operations that are designed to mitigate risks of money laundering.
• Performing know your customer (“KYC”) procedures on all customers.
• Designating a Compliance Officer with full responsibility for the AML Program.
• Providing AML training to all employees.

1. Verification procedures One of the international standards for preventing illegal activity is customer due diligence (“CDD”). According to CDD, Gecobit OÜ establishes its own verification procedures within the standards of anti-money laundering and “Know Your Customer” frameworks.

1.1. Customer identification Gecobit OÜ identifies the customer by obtaining a range of information about him/her. The verification of the identity consists of verifying some of this information against documents or information obtained from a reliable source which is independent of the customer. At least the following information must be received for identification purposes: name and surname; personal identity number (if such exists); date of birth; photograph on an official document which confirms his/her identity; residential address; the number of the personal identification document; the expiry date of the identification document. Gecobit OÜ will take steps to confirm the authenticity of documents and information provided by the customers. All legal methods for double-checking identification information will be used and Gecobit OÜ reserves the right to investigate certain clientss who have been determined to be risky or suspicious. Gecobit OÜ reserves the right to verify clients identity in an on-going basis, especially when their identification information has been changed or their activity seemed to be suspicious (unusual for the particular client). In addition, Gecobit OÜ reserves the right to request up-to-date documents from the clients, even though they have passed identity verification in the past. Clients identification information will be collected, stored, shared and protected strictly in accordance with theGecobit OÜ’s Privacy Policy and related regulations. Once the clients identity has been verified, Gecobit OÜ is able to remove itself from potential legal liability in a situation where its Services are used to conduct illegal activity.

1.2. Sanctions We have integrated with a leading electronic data provider to fulfil the regulatory obligations in line with the EU financial sanctions regime. Information is aggregated from the most important sanction lists (OFAC, EU, UN, BOE, FBI, Bureau of Industry and Security etc.) worldwide and is grouped into one category

1.3. Politically exposed persons In addition to the aforementioned measures, we are integrated with the largest database of Politically Exposed Persons (PEPs), as well as those of their family members. Whenever a client has been identified as a PEP, enhanced

due diligence measures are applied, senior management approval is necessary for establishing or continuing, a business relationship with such a customer.

2. Compliance Officer The Compliance Officer is the person, duly authorized by Gecobit OÜ, 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 Gecobit OÜ's anti-money laundering and counter-terrorist financing, including but not limited to: a. Collecting customers' identification information. b. 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. c. Monitoring transactions and investigating any significant deviations from normal activity. d. Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs. e. Updating risk assessment regularly. f. 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.

3. Transaction monitoring Gecobit OÜ has an ongoing live transaction monitoring process for the purpose of detecting suspicious activity. As advised by the regulator, Gecobit OÜ does not rely solely on a set of prescriptive rules and thresholds; instead, it uses a risk-based approach, both in alert generation and prioritization. The solution utilizes statistical and analytical techniques to identify patterns of unusual and suspicious behaviors by building profiles on each individual customer and comparing their financial activity against expected and/or peer group norms. This is accomplished by using several powerful data analytics tools for flagging anything that falls outside of "normal." We reserve the right to refuse to process a transaction at any stage. Especially, when we believe that a transaction is connected in any way to money laundering or any other type of criminal activity. In accordance with the Estonian law, we are not obliged to inform the customer that it was reported to the corresponding bodies of the customer's suspicious activity.

4. Reporting Gecobit OÜ has established a way in which its staff consults with their line managers to provide evaluation for the rationale of the further disclosure; by no means, this prevents contacting the nominated officer directly. All internal reports are registered in an appropriate way; the nominated officer maintains a secure suspicious report register. The framework is created in such a way, where a reasonable and faithful evaluation is provided to each report that is received. The nominated officer assesses the risk that is posed by a transaction or activity. In cases where there are associated accounts, an examination of such relationships is to be carried out. If an internal review has indicated enough grounds to know or suspect that any benefit has been acquired and if a criminal property exists, an external SAR report is submitted to NCA in a timely manner.

5. Record keeping Records must be kept of all customers' identity, the supporting evidence of verification of identity (in each case including the original and any updated records) and details of any occasional transactions. As per regulatory requirements, we keep records for at least five years from the date a business relationship ends or from the date of the last transaction.

6. Risk Assessment Gecobit OÜ, 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,Gecobit OÜ is able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate to the identified risks. This will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention