ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING POLICY

1. GENERAL FRAMEWORK

This Policy is adopted by ETIS TECHNOLOGIA CONSULTING DIŞ TİCARET LİMİTED ŞİRKETİ (hereinafter, "ETIS" or "the Company"), a Turkish private limited liability company (Limited Şirket) with registered office in İstanbul, Turkey, and operating primarily in the digital crowdfunding sector.

ETIS operates under Turkish Law and complies with the applicable legislation, in particular:

- Law No. 5549 on the Prevention of Laundering Proceeds of Crime (Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun);
- Law No. 6415 on the Prevention of the Financing of Terrorism (Terörizmin Finansmanının Önlenmesi Hakkında Kanun);
- The relevant regulations and guidelines issued by MASAK (Mali Suçları Araştırma Kurulu - Financial Crimes Investigation Board).

The present Policy is binding on all Company employees, partners, collaborators, and third-party service providers who operate on behalf of or in cooperation with ETIS.

The laundering of proceeds from illegal and criminal activities is one of the most serious forms of crime in the financial markets and is an area of specific interest for organized criminal activities.

Money laundering has a significant negative impact on the entire economy: reinvesting illegal proceeds in legal activities and collusion between individuals or financial institutions and criminal organizations deeply affect market mechanisms, undermine the efficiency and fairness of financial activities and have a weakening effect on the economy. Financing terrorist activities may involve using legally derived proceeds and/or criminally derived proceeds. The changing nature of money laundering and terrorist financing, also facilitated by the continuous evolution of technology, requires a constant adaptation of the prevention and contrast measures.

The Anti-Money Laundering (AML) and Counter Financing Terrorism (CFT) regulatory framework is based on a comprehensive set of National and international regulatory sources. As part of the fight against the proliferation of weapons of mass destruction, the United Nations prepared a set of measures to combat financing of proliferation programs, including the prohibition to assist or finance any persons involved in such activities.

Standards are to be considered complementary and applicable since they are not in conflict with the provisions issued by the local Authorities.

ETIS implements the above regulations in its internal regulatory documents. At a general level, the Company has adopted this "Policy on combating money laundering and terrorist financing" (hereinafter the "Policy") as an expression of its commitment to combat the aforementioned criminal phenomena on an international basis, paying particular attention to contrast, in the awareness that the pursuit of profitability and efficiency must be combined with the continuous and effective monitoring of the integrity of corporate structures. The current Policy was approved by the ETIS Company's Board of Directors.

ETIS is committed to complying with this regulatory framework as well as any implementing provisions issued by the Turkish authorities on customer due diligence, data and information retention, organization, procedures, controls and enhanced controls against the financing of programs aimed at the proliferation of weapons of mass destruction. ETIS is thoroughly committed to ensuring that operational organization and the control system are complete, adequate, functional and reliable for strategic supervision, to protecting the Company from tolerance or admixture of forms of illegality that can damage its reputation and affect its stability.

2. METHODS OF IMPLEMENTATION

ETIS operates a digital platform through which private clients may voluntarily allocate funds to projects classified as crowdfunding initiatives. In return for the amounts transferred to the platform, users receive digital utility tokens (hereinafter, "Coin"). The Policy is intended also for the Parent Company and all Group Companies.

The Group Companies implement the Policy by resolution of their own Managing Boards, aligning responsibilities, processes and internal rules with respect to their own structure and size.

All the restrictive measures established to counter the financing of terrorism and all the illicit or suspicious activities that threaten international peace and security can be either commercial, such as import/export restrictions from/to a Country, or financial, such as the partial or total blocking of funds transfer but also operational limitations and freezing of funds.

Restrictive measures include international financial sanctions, also referred to as embargoes, implemented by the Turkish State, foreign agenzie, and supranational organizations (UN, EU). Certain restrictive measures (sanctions) are imposed to all the UN Member States by the Council to implement the Resolutions adopted by the UN Security Council under Chapter VII of the UN Charter. On an international level, there are regulations that establish specific prohibitions or restrictions on investing in certain industrial sectors or importing/exporting from/to “high or significant risk Countries”.

The main requirements set forth by the described regulatory framework are therefore:

- obligation to adopt consistent and coherent procedures for analysis and evaluation of the risks related to money laundering and terrorism financing and establish supervision, controls and procedures needed to mitigate and manage those risks;

- customer due diligence, through which the Company acquires and verifies information regarding the identity of a customer and any beneficial owner, as well as the purpose and intended nature of the relationship or of the transaction, whilst ensuring the constant monitoring of all transactions undertaken by the customer;

- a risk-based approach, whereby customer due diligence obligations are divided into different degrees of due diligence commensurate with the customer's risk profile;

- obligation to retain documents, data and information in order to allow their timely acquisition, transparency, completeness, inalterability and integrity, and an overall and prompt accessibility;

- reporting of suspicious transactions;

- refraining from entering into any new customer relationship, conducting occasional transactions or maintaining an existing customer relationship where due diligence has not been conducted or it is suspected that there may be a link to money laundering or terrorist financing;

- adopting appropriate staff training programs to ensure the implementation and proper application of laws and regulations;

- obligation to disclose any breaches or infringements that may come to the attention of the Control Bodies in carrying out their tasks;

- obligation to adopt procedures to manage internal reporting of violations submitted by employees (Whistleblowing).

3. CLIENT VERIFICATION AND DUE DILIGENCE

Obligations deriving from the national regulatory framework for the prevention of money laundering and terrorism financing require ETIS to:

- adopt appropriate organisational structures, procedures and internal control measures;

- perform “customer due diligence” with a risk-based approach;

- retain data and information;

- report suspicious transactions;

- apply restrictions on the use of cash and bearer securities, applicable to all subjects.

ETIS requires mandatory identity verification (KYC) for all users who intend to:

- Contribute funds to a crowdfunding initiative;

- Receive or utilize Coin;

- Participate in trading, pooling or other functionalities available on the platform.

The Company collects personal identification data, verifies the source of funds when appropriate, and reserves the right to reject or block accounts in case of anomalies, inconsistencies, or suspected illicit activity.

ETIS undertakes all customer due diligence measures when:

- establishing business relations;

- performing occasional transactions, arranged by customers, such as wire transfers or other transactions equal to or above the applicable designated threshold, regardless of whether the transaction is carried out in a single operation or in several related operations or that it consists of a transfer of funds, exceeding the legal limits;

- there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or designated threshold that may apply;

- there are doubts about the veracity or adequacy of previously obtained customer identification data.

In cases where the Bank uses remote identification methods as permitted by law, it adopts special procedures for carrying out its due diligence obligations, also in view of the risk of fraud associated with identity theft. In all cases, the remote identification process involves collecting the customer's and any executor's identification data in electronic format, as well as performing verifications and checks on the authenticity of the data. However, the customer due diligence measures adopted by the Company do not automatically prevent or deny access to financial services for high-risk customers or entire categories of highrisk customers who would be entitled to such access under the applicable regulations.

4. EXTERNAL INTERACTIONS

ETIS issues and manages Coin exclusively for internal use within its platform. ETIS has no responsibility nor control over any external platform, exchange, or broker which may, without authorization, allow for: - Transfer or trading of Coin; - Attribution of speculative value to Coin; - Listing of Coin on third-party marketplaces. The user acknowledges that any use of Coin outside of the ETIS platform occurs entirely at their own risk, without any guarantee, representation or liability by ETIS. As well the Company acts as an intermediary platform that allows users to finance defined projects. Once the crowdfunding initiative has reached its funding goal, the corresponding funds are allocated to independent project operators or contractors. ETIS does not retain control over: - The execution of the project post-funding; - The commercial or financial outcomes of such projects; - The fulfilment of any implicit or explicit expectation by the users.

5. SUSPICIOUS TRANSACTION MONITORING AND REPORTING

ETIS actively monitors activity on its platform for the purpose of identifying potential suspicious transactions. If any operation is suspected to be related to money laundering, financing of terrorism, or other financial crime, the Company will:

- Immediately freeze the relevant operation;

- Retain all user data and transaction evidence;

- Report to the Financial Crimes Investigation Board (MASAK), as required by Law No. 5549.

The Company refrains from establishing, executing or continuing the relationship, operations and professional services (so-called abstention obligation) in the event of an objective impossibility to carry out customer due diligence, assessing whether to report a suspicious transaction. In those cases, in which abstention is not possible, as there is a legal obligation to execute the operation which cannot be postponed or if to decline it could hinder the investigation, the Company is

nonetheless obliged to report the suspicious transaction immediately. Moreover, if after further evaluation or downstream of the enhanced due diligence process, elements of high risk emerge which could affect the legal and/or reputational profile of the Company, ETIS reserves the right to limit or terminate the business relationship with the customer or third party. These limitations may concern i.e., customer or third party access to certain types of products or result in the interruption of services offered by Company in connection with the account/relationship.

The Company has put in place procedures and processes to monitor, identify and report suspicious activities in accordance with the timing and methods required by applicable Law. Employees promptly report any knowledge or suspicion of money laundering, terrorist financing or other criminal activities, or proceeds from criminal activities, regardless of their size, in accordance with the updated organizational model and operating modes provided in reference internal regulation. Until the reporting process is complete, the Company refrain from executing the transaction, unless that is impossible as there is a legal obligation to accept the deed or the execution of the operation cannot be postponed due to the normal conduct of business or where it might obstruct investigations. In these cases, the report is submitted immediately after the transaction has been executed. Grounds for suspicion include the characteristics, scale and nature of the transaction and any other circumstance whatsoever which comes to the employees' knowledge as a result of their duties, also taking into account the financial scope and nature of the business carried out by the subject of the suspicious transaction, as understood from the information acquired by the Company as a result of its activities.

To limit ETIS's risk of involvement – even if unintentional – in the illegal activities mentioned above, an enhanced due diligence process is activated in fund transfer arrangements where the players involved in this type of transaction (originator, beneficiary, the banks involved in the fund transfer) may lead to the suspicion of money laundering, terrorist financing or violations of applicable international restrictions on certain goods, persons or entities. Downstream of the reporting process, ETIS may limit and/or interrupt the business relationship with customers or the third parties, in particular where said relationship may constitute a significant legal or reputational risk.

6. UPDATES AND PUBLICATION

This Policy is reviewed on an annual basis or as required by changes in Turkish legislation. The current version is publicly available on the ETIS website and may be provided to financial institutions or partners upon request.