AML/CFT POLICY

Last updated: 18.12.2025

WE WARN OUR CLIENTS AGAINST ATTEMPTS TO USE OUR SERVICES TO LEGALIZE (LAUNDER) CRIMINAL PROCEEDS, PURCHASE PROHIBITED GOODS AND SERVICES, FINANCE TERRORISM, EXTREMISM, PROLIFERATION OF WEAPONS OF MASS DESTRUCTION, FRAUD, SANCTIONS CIRCUMVENTION AND ANY OTHER ILLEGAL ACTIVITIES. WE ALSO WARN OUR CLIENTS AGAINST ATTEMPTS TO CONCEAL INFORMATION LINKING THEM TO INDIVIDUALS, ENTITIES, ORGANIZATIONS OR COUNTRIES ON THE SANCTIONS LISTS.

This AML/CFT Policy (hereinafter – the Policy) establishes the rules and procedures for countering the financing of terrorist activities and money laundering, which are adhered to by Limited Liability Company “Digital business solutions” (hereinafter – the “Company”, we, us, our, ours) – a legal entity established and operating under the laws of the Kyrgyz Republic: registration number 313924-3301-OOO, TIN 00603202510266, OKPO 33716191, located at the address: 79/4 Isanov Street, Bishkek, Kyrgyz Republic.

This Policy is developed in accordance with and in pursuance of Law of the Kyrgyz Republic dated August 6, 2018 No. 87 “On Countering the Financing of Terrorist Activities and Legalization (Laundering) of Criminal Proceeds” and other regulatory legal acts of the Kyrgyz Republic adopted under this law.

The Company is firmly committed to preventing the use of its services to commit crimes, legalization (laundering) of criminal proceeds or any activity that facilitates legalization (laundering) of criminal proceeds, financing of terrorist, extremist or other criminal activities, as well as financing of proliferation of weapons of mass destruction.

This Policy applies to all the Company's Clients and all services provided by the Company through its facilities – Telegram bot @Swapsterbot or Swapster mobile application.

Before using the Company's services, please read this Policy carefully. If you disagree with any part of this Policy, we kindly ask you not to use the Company's services.

TERMS AND DEFINITIONS

Terms used in this Policy have the following meaning:

Beneficial owner – an individual(s) who ultimately (through the chain of ownership and control) directly or indirectly (through third parties) controls the Client or an individual on whose behalf or in whose interests a transaction (deal) is made;

Verification – a procedure for verifying the identification data of the Client and/or beneficial owner;

Virtual Asset – a set of data in electronic digital form, which has a value, is a digital representation of value and/or a means of certifying property and/or non-property rights, which is created, stored and circulated using distributed registry technology or similar technology and is not a monetary unit (currency), means of payment and security;

High-risk countries – states and territories (entities) that do not apply or insufficiently apply international standards on combating money laundering, financing of terrorism and financing of proliferation of weapons of mass destruction, as well as offshore zones;

Business Relationship – a relationship between the Client and the Company, which has arisen on the basis of an agreement (oral or written) on the provision of services to carry out an operation (transaction);

Freezing of operation (transaction) and/or funds – prohibition to conduct operation (transaction) with funds or transfer, alienation and movement of any funds;

Identification – a procedure for establishing identification data about the Client and/or beneficial owner;

Client – a natural person with whom the Company establishes or has established business relations;

Virtual Asset Wallet – a means (software application or other mechanism/carrier) for storing and transferring a virtual asset;

Legalization (laundering) of criminal proceeds – making the possession, use or disposal of criminal proceeds lawful by means of any actions (operations or transactions) on transformation (conversion) or transfer of property, if it is known that the property represents the proceeds of crime, in order to conceal or disguise the criminal source of origin of the property or to assist a person involved in the commission of a crime in order to evade responsibility for the acts; or conceal or disguise the true nature and nature of the criminal proceeds of crime; or to conceal or disguise the true nature and nature of the criminal proceeds of crime;

Operations (transactions) – any operations (transactions) with funds made to establish, change or terminate civil rights and obligations with funds;

Criminal income – income (funds) received or extracted directly or indirectly as a result of committing a crime in the territory of the Kyrgyz Republic or a foreign country;

Politically exposed persons – one of the following natural persons:

- foreign public official – a person who performs or has performed significant government or political functions (public functions) in a foreign state (heads of state or government, top officials in the government and other state bodies, courts, armed forces, state enterprises, as well as prominent political figures, including prominent figures of political parties);

- national public official – a person who holds or has held a political and special public office or a political municipal office in the Kyrgyz Republic provided for by the Register of public and municipal offices of the Kyrgyz Republic approved by the President of the Kyrgyz Republic, as well as top management of state corporations, prominent political figures, including prominent figures of political parties;

- public official of an international organization – the highest official of an international organization who is or has been entrusted with an important function by an international organization (directors, deputy directors and members of the board of an international organization or persons holding equivalent positions in an international organization);

Risk-based approach – application of enhanced measures in the presence of a high level of risk or simplified measures in the presence of a low level of risk in accordance with established risk management procedures (identification, assessment, monitoring, control, risk mitigation);

Sanctions List – a list of individuals, legal entities, groups and organizations with respect to which there is information about their participation in terrorist or extremist activities and proliferation of weapons of mass destruction. In the Kyrgyz Republic, the Consolidated Sanctions List of the Kyrgyz Republic and the Consolidated Sanctions List of the UN Security Council are used;

Funds – monetary funds and virtual assets;

Internal Control Program – internal measures, procedures and control systems applied by the Company in order to comply with the legislation of the Kyrgyz Republic in the field of countering the financing of terrorist activities or legalization (laundering) of proceeds of crime;

Risk – the risk of financing of terrorist activities and legalization (laundering) of proceeds of crime;

Financing of proliferation of weapons of mass destruction – provision or collection of funds or provision of financial services with the knowledge that the funds are intended or will be used in full or in part to finance the proliferation of nuclear, chemical and biological weapons and/or means of their delivery;

Financing of terrorist activities – provision of funds, provision of financial services or fundraising by any method or means, directly or indirectly, with the intention or awareness that the funds are intended or will be used in full or in part to finance a terrorist and/or terrorist organization or to finance the organization of preparation or implementation of terrorist activities in the Kyrgyz Republic or abroad, or to finance travel of persons sent to the Kyrgyz Republic or abroad;

Financing of extremist activities – provision of funds, provision of financial services or fundraising by any method or means, directly or indirectly (through third parties), with the intention or awareness that the funds are intended or will be used in full or in part to finance the organization of preparation or implementation of extremist activities in the territory of the Kyrgyz Republic.

PROHIBITED ACTIVITIES

The Company does not establish business relations with Clients, suspends rendering of any services to Clients and immediately freezes operations (transactions) and/or funds of Clients for an indefinite period of time without their prior notification in case of suspicion that its services may be used by Clients for legalization (laundering) of criminal proceeds, financing of terrorist and extremist activities, financing of proliferation of weapons of mass destruction and other illegal activities.

In particular, the Company shall immediately suspend operations (transactions) performed by the Client included in the List of persons, groups, organizations in respect of which there is information about their participation in money laundering.

Operations (transactions) will be suspended until the decision to seize the Client's funds is made in accordance with the criminal procedure legislation of the Kyrgyz Republic.

The Company does not establish business relations and does not provide its services to the Clients included in the sanctions lists.

If it is determined that a person is included in the sanctions list, the Company:

- suspends the provision of any services to such Client,
- immediately freezes operations (transactions) and/or funds of such Client without his/her prior notice for an indefinite period of time, until such person is removed from the sanctions list.

The Company does not open anonymous wallets or wallets with knowingly fictitious names.

PROHIBITED JURISDICTIONS

In accordance with our Policy, the Company does not currently work with Clients from the following high-risk jurisdictions:

Algeria, Anguilla, Angola, Antigua and Barbuda, Aruba, Belize, Bermuda, British Virgin Islands, Burkina Faso, State of Libya, Democratic Republic of the Congo, Democratic Republic of the Congo, Gabonese Republic, Grenada, Guinea-Bissau, Islamic Republic of Afghanistan, Islamic Republic of Iran, Kenya, Principality of Andorra, Venezuela, Yemen, Côte d'Ivoire, Democratic People's Republic of Korea, Lao People's Democratic Republic, Lebanon, Macao, Maldives, Monaco, Monaco, Montserrat, Mozambique, Namibia, Independent State of Samoa, Nepal, Niue (New Zealand), Cayman Islands, Cook Islands, Labuan Islands, Turks and Caicos Islands, Republic of Haiti, Republic of Vanuatu, United Republic of Tanzania, Republic of Iraq, Republic of Cameroon, Republic of the Congo, Republic of Mali, Republic of Mali, Republic of the Marshall Islands, Republic of Mali, Mauritius, Republic of Nauru, Republic of Panama, Republic of the Seychelles, Republic of the Union of Myanmar, Republic of the Sudan, Republic of South Sudan, Saint Lucia, Saint Vincent and the Grenadines, Republic of South Sudan, Syrian Arab Republic, Vanuatu, Socialist Republic of Vietnam, Central African Republic, Federal Republic of Nigeria, Federal Republic of Somalia, Federation of Saint Kitts and Nevis, Republic of South Africa, European Union, United States and its territories (Puerto Rico, American Samoa, Guam, Northern Mariana Islands and the U.S. Virgin Islands (St. Croix, St. John and St. Thomas).

The list of prohibited jurisdictions is not final and is subject to change at any time at the Company's discretion and subject to legal and regulatory considerations. If it is found that the Client has provided false information about his/her location or place of residence, the Company reserves the right to take any appropriate action in accordance with applicable laws and regulations, including immediate termination of services to the Client and freezing of the Client's operation(s) (transaction(s) and/or funds. The Client is obliged to inform the Company at the earliest opportunity that he/she has become a resident of any of the above prohibited countries.

POLITICALLY EXPOSED PERSONS

The Company shall use all reasonable means to determine whether the Client, any related party of the Client or any beneficial owner of the Client is a politically exposed person or a family

member (spouse and children, including adopted children) of a politically exposed person or an immediate family member of a politically exposed person (close relatives, business partners and official representatives).

The Company's services to politically exposed persons may and shall be provided only after conducting enhanced due diligence on such persons, including identifying the source of funds and other assets of such persons or any beneficial owner of such persons, as well as obtaining the approval of the Company's management to establish or continue business relations with such persons.

Throughout all business relationships with politically exposed persons, the Company carries out continuous and in-depth monitoring of such business relationships and any operations (transactions) of such persons.

Similar in-depth measures are applied to family members and close persons of a politically exposed person, as well as to other Clients with a high risk level.

MEASURES

In order to prevent the use of the Company's services and facilities for committing crimes, legalization (laundering) of criminal proceeds or any activity that facilitates legalization (laundering) of criminal proceeds or financing of terrorist, extremist or other criminal activities, the Company applies the following measures:

- conducts due diligence of Clients;
- develops and implements an internal system for assessing the level of risks of Clients and their activities, as well as determines a minimum set of requirements, procedures, mechanisms, reports, systems and controls for risk management, and applies stricter procedures in relation to Clients and operations with a high level of risk;
- applies a risk-based approach and assesses the risks of the Company, its partners, and Clients, and classifies Clients based on risk criteria;
- takes enhanced or simplified measures of due diligence of the Client taking into account the results of the Client's risk assessment;
- documents the information obtained as a result of identification and verification of the Client and the beneficial owner;
- implements and regularly updates the internal control program aimed at mitigating the risks of money laundering and terrorism financing;
- continuously monitors the Client's operations (transactions) and their compliance with the available information on the content of the Client's activities, his/her financial position and source of funds, as well as the existence of risks of terrorist financing and money laundering;
- reports suspicious transactions to the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic;
- conducts regular training of employees in the field of AML/CFT;

- conducts a periodic audit of the adequacy of risk level assessment systems, procedures, mechanisms, reports, systems and controls for risk management, as well as the internal control program;
- maintains and updates information and documents on the Client, its financial position, operations (transactions) performed by the Client, as well as information and documents obtained as a result of the Client's due diligence.

CLIENT DUE DILIGENCE

In accordance with the requirements of the current legislation, the Company is obliged to conduct due diligence of all its Clients. As part of the due diligence of Clients, the Company performs the following activities:

- identifies Clients and verifies the information provided by them with the help of reliable, independent sources, and uses the information obtained in assessing the risks associated with the Clients;
- confirms the authenticity of documents and information provided by Clients;
- requests additional information about the Clients and beneficial owners for deep understanding of the risk of their possible involvement in criminal activities;
- -establishes the purpose and intended nature of the business relationship and the source of the Clients' funds to ensure that such funds are not the proceeds of criminal activity;
- investigates Clients whose activities have been identified as suspicious or risky;
- regularly updates Client and beneficial owner identification data using a risk-based approach;
- if necessary, requests additional information from Clients explaining the reasons or economic sense of planned or performed operations (transactions);
- performs enhanced monitoring of business relations with the Client by means of daily monitoring of operations (transactions) and analysis of available information in order to identify signs of suspicious operations (transactions) and operations (transactions) that have no obvious economic sense or obvious legitimate purpose.

DOCUMENTS AND INFORMATION REQUESTED FROM CLIENTS

In order to conduct due diligence on Clients, the Company may request the following documents and information:

- surname, first name, middle name (if applicable);
- date of birth;
- country of residence/citizenship;
- residential address and a document confirming the residential address;
- e-mail address;

- telephone number;
- a copy of a state-issued ID card/passport;
- source of origin of funds and virtual assets.

The Company reserves the right to request any additional documents and/or information at any time.

The Client is obliged to provide the Company with the requested information and/or documents for due diligence. In case the Client fails to provide the information and/or documents required for due diligence of the Client, the Company shall have the right to:

- refuse to establish business relations with the Client;
- suspend or terminate the established business relations with the Client and provision of services to him/her;
- refuse to carry out an operation (transaction).

The Client shall promptly notify the Company of any changes in his/her identification information to ensure the relevance, accuracy and completeness of the provided identification information. The Client is responsible for ensuring that any identification information and supporting documents provided by the Client are current and valid.

MONITORING

The Company continuously monitors the business relationship with the Clients and scrutinizes the operations (transactions) carried out by the Client to ensure that the operations (transactions) are consistent with the information the Company has about the Client, his/her business and risk profile, and, if necessary, the source of funds.

Within the framework of monitoring, the Company performs the following actions:

- verifies operations (transactions);
- requests, if necessary, documents to update/confirm the information obtained during due diligence of Clients;
- finds out the source of the Client's funds;
- conducts in-depth verification of operations (transactions) and regularly updates identification data of Clients with a high risk level.

DETECTION OF SUSPICIOUS TRANSACTIONS

The Company pays special attention to all complex, unusually large or unusual patterns of operations (transactions) carried out by the Client that have no obvious or apparent economic or legal purpose.

If the Company discovers suspicious operations (transactions), it may request from the Client any additional documents and information that may be necessary to clarify the reasons and purposes of such operations (transactions) and document its findings in order to provide this information to the relevant authorities, if the need arises.

In case the Client has not provided information and explanation about a suspicious operation (transaction), a full set of requested documents or submitted suspicious or unusual documents that the Company cannot verify, and the Company reasonably suspects that the Client's actions may be related to legalization (laundering) of criminal proceeds, financing of terrorist or extremist activities or other illegal activities, the Company reserves the right to immediately suspend the provision of services to such Client,

In this case, receipt of funds from the wallet is possible only in case of a positive response of the State Financial Intelligence Service under the Ministry of Finance of the Kyrgyz Republic after a comprehensive investigation of suspicions of illegal activities.

The Company reserves the right at any time to confirm the Client's identity and request any other information in order to comply with the legislation on countering the financing of terrorist activities.

STORAGE OF INFORMATION AND DOCUMENTS

The Company shall keep the following information and documents:

- information, business correspondence and copies of documents received as a result of due diligence of the Client – at least five years after termination of business relations with the Client;
- information and documents on all performed operations (transactions) – at least five years after the operation (transaction) is completed;
- conclusions or statements on analysis of performed operations (transactions) – at least five years after completion of the operation (transaction);
- information and documents stipulated by the legislation of the Kyrgyz Republic in the field of countering the financing of terrorist activities and legalization (laundering) of criminal proceeds – at least five years after termination of business relations with the Client.

PERSONAL DATA

The Company strives to protect the rights of Clients and the confidentiality of their personal data. The Company collects Clients' personal data only to the extent necessary to ensure proper provision of services to Clients and compliance with the requirements of the legislation on combating the financing of terrorist activities and money laundering.

To familiarize yourself with how the Company collects and processes Clients' personal data, please refer to its Privacy Policy.

EMPLOYEE TRAINING

The Company takes all possible measures to train its employees in order to prevent the Company's involvement in actions aimed at using its services to finance terrorist and extremist activities, financing the proliferation of weapons of mass destruction, legalization (laundering) of criminal proceeds, committing other crimes, as well as circumventing sanctions.

With respect to its own employees and partners, the Company takes all necessary measures to thoroughly analyze and screen all candidates for employment and partners for cooperation to

determine whether their activities and/or reputation do not fall into the category of being exposed to or bearing risks.

COOPERATION WITH LAW ENFORCEMENT AND JUDICIAL AUTHORITIES

In order to counter the commission of crimes, legalization (laundering) of criminal proceeds or any activity that facilitates legalization (laundering) of criminal proceeds, financing of terrorist, extremist or other criminal activities, as well as financing of proliferation of weapons of mass destruction, the Company cooperates with law enforcement and judicial authorities, including, but not limited to:

- providing full and comprehensive responses to incoming inquiries, providing all necessary information;
- freezing of the Client's operation (transaction) and/or funds both by court order and out of court;
- transfer of property by court decision to state authorities or victims without paying compensation to Clients who have violated the legislation;
- assistance to law enforcement and other authorized bodies in the investigation of crimes related to virtual assets, as well as information support upon request;
- comprehensive assistance in the return of stolen funds to their rightful owners.

Any inquiries from law enforcement and judicial authorities should be directed to info@swapster.fi.

SUSPICIOUS ACTIVITY REPORT

Clients may notify the Company if they discover that any wallet may be involved in terrorist financing or money laundering activities by contacting the Company at info@swapster.fi.

LANGUAGE

The Policy may be written in several languages. In case of discrepancies between the versions in different languages, the Russian version will take precedence.

CONTACTS

If you have any questions regarding this Policy or the Company's procedures for countering the financing of terrorist activities and money laundering, please contact us by e-mail at info@swapster.fi or via Telegram @SwapsterSupport. The Company endeavors to respond to your inquiries as quickly as possible.

CHANGES TO THE POLICY

This Policy is current as of the effective date indicated above. The Company may update this Policy at any time in its sole discretion as new risks are identified, new services are introduced and applicable laws change by posting the amended version on https://swapster.fi/, the Telegram bot @Swapsterbot or the Swapster mobile application, including the effective date of the amended version. We ask that you check for updates or changes to the Policy yourself from time to time. Your continued use of the Company's services constitutes your acknowledgement and acceptance of such changes to this Policy.