General Framework

Innovative Solutions GRUP SRL (hereinafter also referred to as “The Company”) has no tolerance for money laundering (ML), financing of terrorism (TF) or any other form of illicit activity. Our policies takes into account the anti-money laundering standards applied in the European Union and worldwide. These policies apply to all employees of the Company, and its Directors. The Company operates from and under the laws of Romania. The Company will use recognized and specialised electronic providers for the technical acquisition of the identity data. These policies are applied together with the help of our business partner Ondato and are supervised by our AML officer.

This document and all underlying policies are prepared in line with provisions, requirements and recommendations of the Money Laundering and Terrorist Financing Prevention Act and the FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Assets Service Providers.

In case of any suspicion of illicit activity including money laundering or terrorism financing activities, or where there shall be any doubt about the veracity of our Clients’ identification data further enhanced due diligence measures shall be undertaken in order to correctly identify the purpose and intended nature of the relationship with the Company.

The following are key elements of our AML/CTF Policy:

- Customer Due Diligence
- Business Client Due Diligence
- Simplified Due Diligence
- Enhanced Due Diligence
- Sector and Jurisdiction Restrictions
- Sanctions
- Politically Exposed Persons
- Risk Assessment
- Ongoing Monitoring
- Record Keeping
- Communication with Competent Authorities
- Suspicious Activity Monitoring and Reporting
- Termination of Services
- Data Retention
- Training
- Policy reviewing
- Cooperation and Information Requests
- KYC and AML User Tiers Policy
- AML and Proof of Funds Levels

Individual Customer Due Diligence

Customer due diligence information comprises the facts about a customer that should enable the Company to assess the extent to which the customer exposes it to a range of risks. It is obtained from the customer before actually establishing the business relationship. The Company also verifies the obtained information against reliable and independent sources.

By collecting and verifying the customer's information (passport or identity card, real time selfie) the Company aims to form a reasonable belief as to the true identity of the customer. The Company must also understand the business of the customer to make sure that the customer does not launder illicit funds through the Company and/or these funds will not be used for TF.

Information, documents and data provided to the Company during identification of the customer are processed in accordance with the Company's Privacy Policy.

Business Client Due Diligence

We require all business clients to undergo proper due diligence or Know Your Business (KYB) checks before using our services. This includes, without limitation:

- A full verification of the business owner, director and the majority shareholders (passport or identity card, real time selfie)
- A high-resolution, clearly readable, non-expired, detailed and verifiable copy of the company incorporation document. This must include details on the ownership of the company, its address, tax number, website, purpose and activities
- A description of the sector and business activities and corresponding online website. The website must be registered under the same entity name as the certificate of incorporation provided
- Details of the bank account of the Client
- A high-resolution, clearly readable, non-expired proof of address document not older than 3 months old. The document must carry the Client's business name and address (recent utility bill or bank statement)
- (Optional, for high risk business clients) A video conference with the account holder/business contact person and/or company Director(s)
- (Optional, for high risk business clients) Further documentation may be required for businesses operating in certain regulated, restricted or high-risk sectors of activity

All documents provided should be true copies of the original. Providing false, forged, modified or documents meant to deceive will be considered fraud and treated as such. All assets derived from fraudulent transactions and/or suspicious activity may be seized and forfeited. Such activity may also be reported to the relevant authorities.

Same as for the Customer Due Dilligence, the Company must understand the business of the customer to make sure that the customer does not launder illicit funds through the Company and/or these funds will not be used for TF.

Simplified Due Diligence

The Company may apply simplified due diligence measures where a risk assessment identifies that, in the case of the jurisdiction, economic sector of activity or amounts transacted the risk of money laundering or terrorist financing is lower than usual.

The application of these measures is permitted to the extent that the Company ensures sufficient monitoring of transactions so that it would be possible to identify any unusual behaviour. Monitoring will include, among others: the transacted amount, the location of the sender, the browser signature, the number of transactions performed by apparently the same individual or using the same pattern.

Enhanced Due Diligence

The Company applies enhanced due diligence measures in order to prevent a higher-than-usual risk of money laundering and terrorist financing. These measures are applied on two distinct scenarios:

Prior to client onboarding:

- After receiving the submitted client information and documents, there are reasonable doubts concerning the accuracy of the submitted data, authenticity of the documents or the true purpose of its business activities
- The client is engaged in a high risk sector or activity
- The client is incorporated in a jurisdiction classified as high risk

After client onboarding:

- When the client processed transactional volume exceed the assigned risk threshold for the client
- If unusual or suspicious patterns of activity are detected
- If a transaction request is not consistent with a client’s stated business activity

Sector and Jurisdiction Restrictions

We do not serve Clients from certain jurisdictions that are deemed too high-risk and/or unwelcoming from a legal or regulatory perspective. We can’t provide services to any client that isn’t legally established, or is offering illegal goods or services in their operating jurisdiction(s).

We don’t accept business partners from the following jurisdictions: Afghanistan, Antarctica, Bahamas, Barbados, Botswana, Bouvet Island, Cambodia, Central African Republic, Congo, Cook Islands, Côte d’Ivoire, Cuba, Democratic People's Republic Of Korea (DPRK), Ghana, Guam, Iran, Iraq, Jamaica, Kosovo, Libya, Mauritania, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Somalia, South Sudan, Sudan, Syria, Trinidad and Tobago, Uganda, Vanuatu, Venezuela, Western Sahara, Yemen and Zimbabwe.

We are also not accepting businesses from the following list sectors and activities:

- Services that collect or exploit natural resources in an overly extractive way
- Any services dealing with nuclear energy or nuclear materials
- Currency sales by non-financial institutions
- Bankruptcy attorneys or entities engaged in the collection of debt
- Credit protection services
- Credit counselling services
- Services that produce, sell or distribute controversial non-revenue substances of any kind for which the regulatory situation is not specifically clear or of a dubious nature
- Any media that promotes or contains incitement to hatred, violence, harmful or inappropriate content (as determined by applicable law)
- Any services involving military equipment and weapons
- Any service, group or organisation promoting or containing incitement to hate, violence, or harmful content
- Escort services
- Fuel stations and dispensers
- Services that may, by association, negatively impact the company's reputation
- Services that use forced or child labor
- Institutions recognized for dealing with shell companies.

Sanctions

The Company may employ automated screening software to identify and block known virtual asset addresses associated with sanctions and numerous illegal and high-risk activity. The company does not do business with companies under sanctions. Sanction lists considered include, among others:

- EU Sanctions
- UN Sanctions
- Sanctions administered by the Office of Foreign Assets Control (“OFAC-US”).

All verified matches are automatically blocked and the matter escalated to a Compliance Officer for further analysis and appropriate actions.

Politically Exposed Persons

Politically Exposed Persons (“PEP“, a natural person who is or who has been entrusted with prominent public functions, as well as their families and persons known to be close associates) are required to be subject to enhanced scrutiny by reporting entities. According to the Financial Action Task Force a PEP may be in a position to abuse their public office for private gain and may use the financial system to launder the proceeds of this abuse of office.

The PEP definition and classification applies to the beneficial owners of the business as well and may constitute an additional factor of risk.

Politically Exposed Persons will not be allowed to onboard the platform.

Transaction Monitoring

When a transaction starts we are logging the IP address and the values stored in a cookie and in the local storage. An automatic mechanism detecting repeating transactions coming from apparently the same user (or purchasing the same product at a higher rate than before). Such transactions are temporarily locked and we are notified in order to perform a human screening. Such events are logged for both the purchaser and the seller and, if repeated, can lead to account suspension.

Actions On Transaction Monitoring

LOCKING means full transaction lock and withdrawals freezing for a specific partner, plus a direct notification sent to the AML officer. The AML officer will have to determine if the activity really is suspicious or not beyond any reasonable doubt. All suspicious activities will be reported to authorities (see "Suspicious Activity Monitoring and Reporting"). If the activity that caused the alert proves to be legit it can lead to an increase of the default threshold.

NOTIFICATIONS will only notify our team and raise an internal flag. Failure for the Company employees to contact the seller in order to determine if all sales are justified and legit within 10 (ten) working days will lead to LOCKING.

Transactions coming from IP address associated with sanctioned countries (as provided by our partner Ondato) are automatically denied from the start.

Several thresholds are in place, each of them leading to one or both of the actions described above. For each seller:

- more than 10 orders originating from the same IP address in a 24 hours moving window lead to: notification and lock

- more than 10 orders originating from the same wallet in a 24 hours moving window lead to: notification and lock

- more than 30% increase in order numbers when compared to the previous 24 hours lead to: notification only

- receipt of a cryptocurrency amount more than 20% larger than the defined product price lead to: notification

- increases in product pricing over the equivalent of 150 EUR lead to: notification

Risk Assessment

The Company applies a risk-based approach in order to reduce the risks of money laundering and terrorist financing to which it is exposed. Enhanced measures will be taken in situations where the risks are higher.

The Company will monitor each transaction in detail in order to avoid ML/TF. We take into account several aspects including: the price of the products defined by our clients as well as the IP addresses and browser signatures for each payment, the number of repeated orders and more.

Ongoing Monitoring

The Company performs an ongoing monitoring of the business relationships with customers for both low-risk and high-risk clients depending on each customer's business and provided service.

Ongoing monitoring by both software automation and human screening allows the Company to gain deeper insights into customers' profiles and behaviours.

Additionally, customer data will be periodically reviewed and updated to make sure we have correct and sufficient information. The schedule below will be used:

- every 6-12 months for high-risk customers
- every 12-24 months for standard-risk customers
- and every 24-36 months for customers with low risk

Record Keeping

Record keeping is essential to facilitate effective investigation, prosecution and confiscation of criminal property. Therefore the Company maintains appropriate records in relation to

every customer, with the idea being that maintaining an audit trail is a significant component of combating ML/TF.

Communication with Competent Authorities

The Company will report to the competent authorities and will cooperate on any follow-up actions upon suspicion or any knowledge that the property of any value is directly or indirectly derived from criminal activity or participation in such activity, or that the intended purpose of property is to sponsor illegal activity, terrorism or terrorist organizations.

Suspicious Activity Monitoring and Reporting

Suspicious activity is monitored using both software procedures and human operators. An investigation will try to establish the true motivation behind the activity in question in order to determine if it really is suspicious or remove the reasonable doubt. Suspicious activities will be escalated both internally and externally.

When money laundering, terrorist financing or any other illegal activity is detected the Compliance Officer will determine whether a filing with any law enforcement authority is necessary.

The Company and all its employees, officers and directors are prohibited to inform a person, its beneficial owner, representative or third party about a report submitted on them to the Financial Intelligence Unit, an intention to submit such a report as well as about the commencement of criminal proceedings.

Termination of Services

The company reserves the right to deny or terminate servicing a client or account at any time in line with the terms stipulated in the User Agreement if suspicion arises that a Client is involved with or connected with money laundering, criminal activity, terrorist financing or any other predicate offense to money laundering or terrorist financing.

Data Retention

The Company is obligated to retain all documents and information which served for identification and verification of the client or information concerning a particular customer or transaction (either as an occasional transaction or within a business relationship), for a period of no less than 5 (five) years after termination of the business relationship. The Company will also retain the records of SAR/STR for 5 (five) years from the filing date.

The Company implements necessary rules for the protection of personal data upon application of the requirements arising from its obligations hereunder.

The Company is allowed to process personal data gathered upon implementation of these rules only for the purpose of preventing money laundering and terrorist financing and the data must not be additionally processed in a manner that does not meet the purpose, for instance, for marketing purposes.

Training

It is the Compliance Officer's task to ensure that Company's employees are fully aware of their legal obligations under the AML/CTF standards by introducing a complete training program that aims at educating them on the latest developments in the prevention of ML/TF.

The frequency and content of the training are determined according to the needs of the Company, the amendments of legal and/or regulatory requirements, as well as any changes in the business model. The training frequency will be at least once per year.

Policy reviewing

The Company will review the current AML/CTF policies and procedures regularly, at least once per year.

Cooperation and Information Requests

The Company will cooperate with supervisory and law enforcement authorities in preventing money laundering and terrorist financing. It will communicate information available to the Company and reply to queries within a reasonable time, following the duties, obligations and restrictions arising from legislation. The Company will also comply with Law Enforcement requests for information where it pertains to specific preservation orders and fund freezing.

We will not voluntarily disclose non-public information to a requesting party. In accordance with European Union privacy laws, the company will only disclose non-public user information if it has received consent of the user and in response to a legitimate and an enforceable subpoena, court order or search warrant from a body that has jurisdiction to compel the company to disclose that information. For law enforcement agencies outside of the European Union, procedure under the Mutual Legal Assistance Treaty ("MLAT") may apply.

KYC and AML User Tiers Policy

(applies to both personal and business accounts)

	New account	Identity verified	IBAN verified
Incoming crypto payments below 1000 EUR	X	X	X
Incoming crypto payments of 1000 EUR and above		X	X
Crypto withdrawals		X	X
Exchanges		X	X
Receive affiliate rewards		X	X
FIAT withdrawals			X

AML and Proof of Funds Levels

(applies for direct crypto deposits, not sales, to both personal and business accounts)

	Level 1	Level 2	Level 3	Level 4
Threshold amount	10.000	20.000	100.000	Unlimited
Confirmed email	X	X	X	X
Phone number	X	X	X	X
Pass identity verification	X	X	X	X
FIAT bank statement	X	X	X	X
Document declaring source of funds		X	X	X
Document proving source of funds			X	X
Document proving extended source of funds				X

Additional notes:

- All amounts are in EUR and apply only to FIAT balances.
- For non-EUR balances the amounts are converted to EUR at the daily official exchange rate before adding to your AML limits.
- All threshold amounts are summed up on a per-year basis (ie. for Level 3 you may deposit up to 30,000 in 2022 and again up to 30,000 EUR 2023.

- The threshold amount is counted separately for deposits and withdrawals (i.e. for Level 3 an account and deposit up to 30,000 in crypto and separately withdraw up to 30,000 EUR).
- For the unlimited account at Level 4 based on the documents provided by you a limit will be set by our AML officer. You may ask to increase that limit at any moment, by providing documents for other funding sources.

A Proof of Sources of Funds (POSOF) is a collection of documents that explains where the crypto assets used for a fiat withdrawal originated. Any POSOF document submitted needs to cover all deposits or withdrawals via that particular funding method.

Examples of acceptable POSOF:

- Standardised statement from a digital asset exchange
- Proof of balance at crypto exchange(s)
- Signed message on crypto wallet

For High Limits Only in Level 4:

- If holding wealth on another exchange: an account statement or proof of balances letter
- If holding wealth in a private wallet: sign a message using your cryptocurrency address