AML & KYC Policy

ESAX Technologies Corporation has established an Anti-Money Laundering and Know Your Customer Policy (Hereinafter - The “AML & KYC Policy”), in an attempt to maintain the best compliance practices in conjunction with applicable laws and regulations relating to anti-money laundering in all countries where we operate.

Money Laundering is defined as:

The conversion or transfer of property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person’s actions;

The acquisition, possession or use of property derived from criminal activity or property obtained instead of such property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation therein;

The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property derived from criminal activity or property obtained instead of such property, knowing that such property is derived from criminal activity or from an act of participation in such an activity. Money laundering also means participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the activities referred to above.

Terrorist financing is defined as the financing and supporting of an act of terrorism and commissioning thereof as well as the financing and supporting of travel for the purpose of terrorism both international and local laws and regulations require BITESAX EXCHANGE 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 users.

AML & KYC Policy Covers The Following Areas:

- **Internal Controls**
- **Compliance Officer**
- **Training**
- **Customer Verification Procedures**
- **Monitoring of Transactions**
- **AML Program Audit**

Internal Controls :

We have designed a structured system of internal controls in order to comply with applicable anti-money laundering, countering financing of terrorism (hereinafter - the "AML/KYC") laws and regulations, including, but not limited to:

- Establishing customer's identity and verifying the information provided;
- Establishing special regime for dealing with customers which are politically exposed persons (PEP);
- The identification of unusual activity and facilitating the reporting of suspicious activity (SAR);
- Record keeping of customer documentation and transactional history.

Compliance Officer:

The compliance officer is the person, duly authorized by BITESAX EXCHANGE, whose duty is to develop and enforce the effective implementation of the AML/KYC. The compliance officer is required to report any violations of the AML/KYC procedures and is responsible for collecting and filing sars.

It is the compliance officer's responsibility to supervise all aspects of BITESAX EXCHANGE's anti-money laundering and counter-terrorist financing measures, including but not limited to:

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;

Collecting User's Identification information and verifying the information provided; implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;

Collection and analysis of information referring to unusual transactions or transactions or circumstances suspected of money laundering or terrorist financing, which have become evident; investigating any unusual, suspicious activity;

Reporting to the appropriate authorities in the event of suspicion of money laundering or terrorist financing; providing law enforcement with information as required under the applicable laws and regulations;

Periodic submission of written statements on compliance with the requirements arising from law to the management board;

Organization of the training of employees;

- Performance of other duties and obligations related to compliance with the requirements of law; updating risk assessment regularly.
- The compliance officer is entitled to interact with law enforcement, which are involved in prevention of money laundering, terrorist financing and other illegal activity.

Training:

All employees receive a full AML & KYC training, along with a job-specific guidance. Training is conducted at least once a month to ensure that trainees are informed and act in compliance with all applicable laws and regulations. New employees receive relevant training within thirty (30) days of their start date and before they could perform any compliance related duties. Training program is updated regularly to reflect current laws and regulations. Compliance Officer maintains the training logbook, which is available for verification during the annual third party review.

Customer Verification Procedures:

BITESAX EXCHANGE establishes its own customer verification procedures within the standards of AML & KYC frameworks. In order to open an account, customer's identity and place of residence need to be verified and checked against sanctions and watch lists, including The Office of Foreign Assets Control ("OFAC") nd Politically Exposed Persons list ("PEP"). In addition, certain groups of assets are limited to investors with "qualified" status only. In order to open an account for an individual customer, the following

Information needs to be verified:

- **Email address;**
- **Mobile phone number;**
- **Full name;**
- **Date of birth;**
- **Proof of identity (government identity card, driver's license, passport);**
- **Citizenship;**
- **Proof of residential address (utility bills, bank statement, official government letter); and**
- **Additional information or documentation if requested.**

Based on the information collected during the KYC process the Company have a right, at its own discretion, to restricts or refuse service to a particular client..

Monitoring of Transactions:

BITESAX EXCHANGE carries out customer's transactions monitoring, risk-assessment and suspicious activity detection. For that purpose it uses specially developed system, including using a high-performance tools.

BITESAX EXCHANGE uses risk-based approach to combating/preventing money laundry and/or financing terrorism. To assist in determining the level of AML/KYC due diligence to be exercised with regard to the customer, a compliance risk profile is calculated first of all on entry into relations (low, medium, high), and is then recalculated routinely.

AML/KYC compliance ensures that an ongoing transaction monitoring is conducted to detect transactions which are unusual or suspicious compared to the customer profile.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to The Knowledge of The Customer (KYC), their financial behaviour and the transaction counterparty.

Transaction is inconsistent with a customer's known personal usual activities or personal habits, this transaction may be considered suspicious. data and transaction monitoring tools are used to identify unusual/uncommon patterns of customer's activity. After review and investigation, it is compliance officer's decision whether to file a sar or not.

Once a sar is filed with a relevant agency, a copy of filing documentation is maintained. Sar filing is confidential and only the BITESAX EXCHANGE's employees involved in the investigation and reporting process will be aware of its existence.

All records are retained for no less than (5) years and are available upon official request by an authorized examiner, regulator, or law enforcement agency.

Any BITESAX EXCHANGE staff member must inform the compliance officer of any atypical transactions which they observe and cannot attribute to a lawful activity or source of income known of the customer.

Aml Audit :

The compliance officer is responsible for conducting AML/KYC audit at least annually. Other audit demands are set in internal policies and procedures.

We apply due diligence measures, in particular:

- Upon establishment of a business relationship;
- Upon verification of information gathered while applying due diligence measures or in the case of doubts as to the sufficiency or truthfulness of the documents or data gathered earlier while updating the relevant data;
- Upon suspicion of money laundering or terrorist financing;
- In some other cases, including in other exact cases prescribed by law and in cases of identifying "Red Flags" in accordance to internal procedures.

Preservation of Data:

We retain the originals or copies of the documents, which serve as the basis for identification and verification of persons, and the documents serving as the basis for the establishment of a business relationship no less than five years after termination of the business relationship.

We retain the documents prepared with regard to a transaction on any data medium and the documents and data serving as the basis for the notification obligations for no less than five years after making the transaction or performing the duty to report.

Our monitoring of a business relationship includes, in particular:

- Checking of transactions made in a business relationship in order ensure that the transactions are in concert with our knowledge of the customer, its activities and risk profile;
- Regular updating of relevant documents, data or information gathered in the course of application of due diligence measures;
- Identifying the source and origin of the funds used in a transaction;
- Paying more attention to transactions that a likely to be linked with money laundering or terrorist financing, including to complex, high-value and unusual transactions and transaction patterns that do not have a reasonable or visible economic or lawful purpose or that are not characteristic of the given business specifics;
- Paying more attention to the business relationship or transaction whereby the customer (or payment provider, etc. of the customer) is from a high-risk third country or a country or territory specified by law as country or jurisdiction with factor(s) increasing the geographical risk.