

AML/CFT/KYC POLICY

ARTESSERE GmbH, Switzerland (hereinafter - the "ARTESSERE") Anti-Money Laundering, Countering Financing of Terrorism and Know Your Customer Policy (hereinafter - the "AML/ CFT/KYC Policy") is designated to prevent and mitigate possible risks of ARTESSERE (artessere.com) being involved in any kind of illegal activity.

Both international and local regulations require ARTESSERE 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.

"Money laundering" means: 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 counseling the commission of any of the activities mentioned above.

"Terrorist financing" means 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.

AML/CFT/KYC Policy covers the following matters:

- Internal Controls;
- Training;
- Compliance officer;
- Verification procedures;
- Risk Assessment;
- Monitoring of transactions;
- AML Program Audit.

Internal Controls

We have created a structured system of internal control and procedures in order to comply with applicable AML/CFT laws and regulations, including, but not limited to:

Training

- verifying users' identity and the information provided;
- the identification of unusual activity and suspicious activity reporting (SAR);
- keeping records of Users' documentation and transactional history.

All the appropriate employees regularly pass a full AML/CFT training, along with a job-specific guidance. Training is conducted to ensure that trainees are informed and act in compliance with all applicable laws and regulations. New employees pass relevant training before commencing to work. Training program is updated regularly to reflect current laws and regulations.

Compliance Officer

The Compliance Officer is the person or external profiled service provider company, duly authorized /having agreement by/with ARTESSERE, whose duty is to ensure the effective implementation and enforcement of the AML/CFT/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of ARTESSERE's anti-money laundering and counter-terrorist financing, 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; implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs; collecting Users' identification information; organization of the 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 significant deviations from normal activity; reporting to the appropriate authorities (Financial Intelligence Unit etc.) 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.

Verification procedures

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

Identity verification

ARTESSERE's identity verification procedure requires the User to provide ARTESSERE with reliable, independent source documents, data or information (national ID, international passport, utility bill or domicile address, W8BEN or

W9 tax form / TIN / UID number etc). For such purposes ARTESSERE reserves the right to collect User's identification information for the AML/CFT/KYC Policy purposes.

ARTESSERE will take steps to confirm the authenticity of documents and information provided by the Users. All legal methods for double-checking identification information will be used and ARTESSERE reserves the right to investigate certain Users who have been determined to be risky or suspicious.

ARTESSERE reserves the right to verify User's 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 User). In addition, ARTESSERE reserves the right to request up-to-date and/or additional documents from the Users while passing verification and even though they have passed identity verification in the past.

User's identification information will be collected, stored, shared and protected strictly in accordance with the ARTESSERE's Privacy Policy and related regulations. While verification procedures users are checked against sanctions and watch lists, including the Office of Foreign Assets Control (OFAC) and PEP list.

Risk Assessment

ARTESSERE, 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, ARTESSERE 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.

Monitoring of transactions

The Users are known not only by verifying their identity (who they are) but, more importantly, by analyzing their transactional patterns (what they do).

Therefore, ARTESSERE performs users' transactions monitoring, risk-assessment, suspicious activity detection and a variety of compliance-related tasks, including

capturing data, filtering, record-keeping, investigation management, and reporting. ARTESSERE reserves the right to use for that special software tools and external services.

System functionalities include: constant check of Users against recognized "black lists", aggregating transfers by multiple data points, placing Users on watch and service denial lists, opening cases for investigation where needed, sending internal communications and filling out statutory reports, if applicable; case and document management.

With regard to the AML/KYC Policy, ARTESSERE will monitor all transactions and it reserves the right to: ensure that transactions of suspicious nature are reported to the proper bodies, law enforcement through the Compliance Officer; request the User to provide any additional information and documents in case of suspicious transactions; suspend or terminate User's Account when ARTESSERE has reasonable suspicion that such User engaged in illegal activity.

The above list is not exhaustive and the Compliance Officer will monitor Users' transactions on a day-to-day basis in order to define whether such transactions are to be reported and treated as suspicious or are to be treated as bona fide. If a transaction is inconsistent with a user's usual activities, this transaction may be considered suspicious. Data and transaction monitoring tools are used to identify uncommon patterns of user's activity.

All records are retained for a term prescribed by applicable law and internal procedures and are available at official request of authorized state body according to law.

AML Program Audit

The Compliance Officer is responsible for conducting AML/CFT audit at least annually. Other audit demands are set in internal policies and procedures.