AML/KYC Policy

Last updated: August 4, 2021

Introduction

Digital System Anti-Money Laundering and Know Your Customer Policy (hereinafter - the "AML/KYC Policy") is designated to prevent and mitigate possible risks of Digital System being involved in any kind of illegal activity.

Both international and local regulations require Digital System 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 matters:

1. Verification procedures
2. Compliance Officer
3. Monitoring transactions
4. Risk assessment

1. Verification procedures

One of the international standards for preventing illegal activity is customer due diligence ("CDD"). According to CDD, Digital System establishes its own verification procedures within the standards of anti-money laundering and "Know Your Customer" frameworks, including enhanced due diligence for customers presenting a higher risk, such as Politically Exposed Persons (PEPs).

Digital System's identity verification procedure requires the User to provide Digital System with reliable, data or information (full name, e-mail, address, etc.). For such purposes Digital System reserves the right to collect User's identification information for the AML/KYC Policy purposes.

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

Digital System 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, Digital System reserves the right to request up-to-date documents from the Users, 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 Digital System's Privacy Policy and related regulations.

Once the User's identity has been verified, Digital System is able to remove itself from potential legal liability in a situation where its Services are used to conduct illegal activity.

2. Compliance Officer

The Compliance Officer is the person, duly authorized by Digital System, whose duty is to ensure the effective implementation and enforcement of the AML/KYC Policy. It is the Compliance Officer's responsibility to supervise all aspects of Digital System's anti-money laundering and counter-terrorist financing, including but not limited to:

- Collecting Users' identification information;
- 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;
- Monitoring transactions and investigating any significant deviations from normal activity;
- Implementing a records management system for appropriate storage and retrieval of documents, files, forms and logs;
- 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.

3. Monitoring 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, Digital System relies on data analysis as a risk-assessment and suspicion detection tool. Digital System performs a variety of compliance-related tasks, including capturing data, filtering, record-keeping, investigation management, and reporting.

With regard to the AML/KYC Policy, Digital System will monitor all transactions and it reserves the right to:

- Ensure that transactions of suspicious nature are reported to the proper 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 Digital System has reasonably 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.

4. Risk assessment

Digital System, 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, Digital System 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.