Information Security Requirements for Digital Financial Asset Exchange Operators

1. The exchange operator of digital financial assets, as defined by the regulations of the information system of Distributed Ledger Systems LLC and Federal Law No. 259-FZ "On Digital Financial Assets, Digital Currency, and Amendments to Certain Legislative Acts of the Russian Federation" dated July 31, 2020 (hereinafter, the **"Exchange Operator"**), ensures the uninterrupted and continuous operation of the information system in which digital financial assets are issued, operated in its part by Distributed Ledger Systems LLC (hereinafter, the **"information system"**).

2. The Exchange Operator must establish and review at least once a year the threshold levels of continuity indicators, based on the results of the information system risk assessment.

3. The Exchange Operator uses a comprehensive set of information protection measures and tools to ensure the necessary level of security for software systems and products, information infrastructure, and to allow for real-time monitoring of the information security state, tracking, and timely responding to events affecting information security.

4. Only up-to-date versions of information protection tools must be used by the Exchange Operator to safeguard information. All information protection tools must undergo an audit at least once every two years. Upon receiving information about new types of threats not accounted for, information protection tools must be updated to fully match the capabilities to counter newly identified threats.

5. The Exchange Operator ensures protection against intrusions by preventing interference from publicly accessible data transmission networks, including the Internet. It conducts analysis and limits (if necessary) the incoming and outgoing data flow to meet the security rules requirements.

6. An information security suite must include the following main components: event logging, data transmission encryption, and access restriction.

   6.1. **Event logging:** continuous recording of all system events for real-time analysis and investigation of incidents and failures.

   6.2. **Data transmission encryption:** personal, identification, and authentication data are transmitted exclusively using encryption, as per regulatory body requirements.

   6.3. **Access restriction:** all information system users, including Exchange Operator employees, receive personalized access using authentication data. A role model is used in which each user has separate authentication credentials to perform different functions depending on their current role. Roles with conflicting interests cannot be assigned to the same user;

7. Interaction with the Exchange Operator must be conducted using secure communication channels.

8. The Exchange Operator implements measures to detect transactions aimed at conducting financial transactions without the consent of information system users, as established by the Bank of Russia.

9. As part of the implementation of user interaction processes, the Exchange Operator takes measures aimed at ensuring information security, including allocating a separate contact for the service responsible for identifying and eliminating incidents and regular assessments of the security level of the software and hardware complex:

   9.1. Allocation of a separate contact of the service responsible for identifying and eliminating incidents, including countering unauthorized operations;

   9.2. Regular, at least annual, security level assessment of the Exchange Operator's software and hardware complex.

10. Within the implementation of user interaction processes, the Exchange Operator undertakes the following measures aimed at ensuring operational reliability:

   10.1. Backup of communication facilities, including communication channels, hardware, and software;

   10.2. Regular testing of backup measures at least once a year;

   10.3. Description of the procedures for the Exchange Operator’s subdivisions to respond to and mitigate abnormal situations during interactions with users of the information system.