Requirements for the Information Security of the Information System Node

1. The node of the information system, 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 Node"**), 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 **"IS"**).
2. The Node must establish and review at least once a year the threshold levels of continuity indicators, based on the results of the IS risk assessment.
3. The Node 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. The Node must use only the latest versions of information protection tools for safeguarding 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 Node 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. **Access restriction**: Users who are employees of the Node 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. The Node implements the following measures directed at ensuring information security:
   7.1. Allocating a dedicated contact within the service (unit) responsible for identifying and addressing incidents;
   7.2. Regularly, at least once a year, assessing the security level of the Node's software and hardware complex.
8. As part of the process of interaction with other IS nodes, the Node implements the following measures aimed at ensuring operational reliability:

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

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

8.3. Describing the procedures for the Node's employees to respond to and address abnormal situations.