

Security Policy

DBX GLOBAL CRYPTO NETWORK ELECTRONIC TRADE AND SOFTWARE

Information security measures used in working with tools and services <https://dbx.so>

Ensuring information security when working with clients at <https://dbx.so> is a top priority when building technological schemes and contractual relations.

The applied information security measures imply continuous improvement by adding and refining new tools to protect information and work with it, improving the audit procedure and reducing the "attack surface" in its own infrastructure.

Actions to protect clients' information and clients' work at <https://dbx.so> are manifested in the implementation of the following complex procedures:

1. Protection of users' accounts and traffic

Some of the following security measures are enabled by default, while other clients working in <https://dbx.so> may connect by themselves, depending on the desired degree of protection.

- two-factor authentication (2FA)

An additional level of account protection and the most important operations in it, such as authorization, API key generation and money withdrawal. Two-factor authentication can be configured with Google Authenticator for a two-step authentication using Google's Time-based one-time Password Algorithm (TOTP) and HMAC-based One-time Password Algorithm (HOTP), or by using **e-mail** to obtain an authorization verification code.

- using HTTPS protocol

HTTPS protocol, working through the encrypted transport mechanism TLS 1.2 provides protection against attacks based on listening to the network connection.

- advanced test instruments to control the integrity of the account

Authorization data is stored and checked for suspicious activity. The

intelligent system keeps track of IP address changes to prevent a work session from being compromised. Notifications are sent by email with reports about the authorization and a reference to the quick freezing of the account if malicious activity.

- restriction on access to the account by IP-address, protection during money withdrawal

The security system monitors the withdrawal of funds by IP-address and other regularities in the user's behavior and initiates a manual check for suspicious output operations by the administrator. The procedure of withdrawal confirmation is resistant to malicious modules in the browser.

The white list of addresses allows you to prevent the withdrawal of funds to third party resources.

System Security

The latest Linux systems are used to host the platform. All the <https://dbx.so> servers use patch management system, continuously verify the system and application software against databases of vulnerabilities, including a database of threats to information security FSTEC, so the <https://dbx.so> servers are protected by the most current software and best practices of computer security.

1. Automatic database backup on a daily basis

Once a day, a backup copy of the trading platform database is created, after which it is encrypted and placed in the archive.

2. Automatic duplication of backup data

The backup created (database, log files, etc.) is immediately sent to multiple physical servers that are remote from each other.

3. Defense from DDoS-attacks

<https://dbx.so> when working uses automatic protection from distributed denial-of-service attacks to prevent external attacks from affecting the course of a trade.

4. Physical and organizational security measures

We are constantly improving the ways of data collection, transfer, storage and processing, including physical security measures, to prevent unauthorized access to our system. The servers are hosted in securely protected data centers, equipped with video surveillance systems and access control systems installed at the racks with servers.

All the employees undergo introduction training on Informational Safety, as well as training on rules and measures of information security regarding the execution of their functional responsibilities with periodic control of their knowledge.

We have strict restrictions on our employees, contractors and agents' access to the personal information, we also impose strict contractual obligations on them, for the violation of which dismissal or sanctions are provided.

Together, the measures described above, aimed at ensuring information security of customers working with products and services at <https://dbx.so> correspond to modern standards and are aimed first of all at the protection of client operations, information on it, as well as of customers' funds.