ICBC

+7 (495) 287-30-99
support@icbcmoscow.ru

RECOMMENDATIONS FOR ENSURING INFORMATION SECURITY WHEN WORKING IN THE DBO SYSTEM

Compliance with these recommendations will ensure maximum security and control of your accounts, reduce possible risks when making electronic payments in the DBO System, and counteract fraud and illegal actions of intruders aimed at stealing funds from your accounts.

1. The Client independently determines the order of accounting, storage and use of key information carriers, SC generators, which should completely exclude the possibility of unauthorized access to them by unauthorized persons.

2.Under no circumstances should anyone, including Bank employees and relatives, share your username and password to log in to the DBO System, or give them the key information carrier or the SC generator. If you receive such a request, please call the Bank back at the phone numbers indicated in these recommendations and inform us about this fact.

3. The Bank, under no circumstances, has the right to demand confidential information from you (including passwords and the content of incoming SMS messages).

4. The login, password, key information carrier, and IC generator must be kept secret from third parties, including Bank employees and relatives. It is recommended to keep the login password and PIN code from the key information carrier separately.

5. The username and password must be remembered or, if this is difficult, stored in an implicit form and inaccessible to third parties, including Bank employees and relatives.

6. Do not send your username and/or password using SMS messages, instant messengers and social networks, as well as by mail or email.

7. Do not enter your access password on sites whose address is different from the site address of the DBO System of ICBC Bank (JSC). Make sure that the address is correct. The establishment of a cryptographically strong Internet connection must be confirmed using a valid Bank ssl certificate. If it is not possible to connect to the DBO System, please report this to the Bank at its address.

8.It is recommended to change the access password to the RBS System regularly, and do not store the password in paper form next to the ARM used for working with the DBO system.

9. Do not follow the links provided in the emails (including links to the Bank's website), as they may lead to phishing duplicate sites (the presence of additional characters in the site address, the content of provocative information, the absence of the name of the site developer, as well as an email address for feedback or a mailbox is specified as the contact address on one of the free email services).

10. Beware of spyware programs that can get into your computer when you open Internet pages containing tempting offers or sensationalism. Pay special attention to the files attached to messages received by email. If you are not sure about their origin, it is better not to open files with the extension .exe., .com., .bat., .pif., .vbs, .vbe, .cmd.

11. Access to computers should be restricted as much as possible only to responsible full-time IT specialists of the Client and only to responsible employees-owners of the item instance. Key information carriers should be assigned to Authorized Persons personally, because only in this case, the Authorized Person is sure of the absolute confidentiality of the EP Key and its inaccessibility even to their colleagues, and is fully aware of the responsibility for the content of the EPDs signed by their EP. Unauthorized persons should be strictly excluded from accessing key information carriers, SC generators, usernames

and passwords. When servicing a computer by IT employees, including non - standard ones who come on a call, perform prevention and Internet connection, install and update accounting and reference programs, install and configure other software on computers that work on the DBO System, ensure control over the actions performed by them.

12. If a responsible employee is dismissed or replaced (including a change in the General Director or chief accountant), as well as any other actions that affect the change in the composition of Authorized Persons who have access to the DBO System, it is necessary to immediately inform the Bank in accordance with the established procedure and block the EDS Keys previously used by these persons. New Item Instance Keys must be generated for new Authorized Persons. In this case, it is also recommended to perform an unscheduled change of the remaining passwords and Code Word.

13. For storing key information carriers in the Client's premises, it is recommended to install metal vaults (safes) equipped with reliable locking devices. Storage of key information carriers is allowed in the same storage with other documents in a separate container, sealed by an Authorized Person.

14. Placement of technical equipment in a room equipped with the Client's automated control system should exclude the possibility of visual viewing of confidential documents and monitor screens on which they are reflected, through windows, etc. openings and video recording devices above the workplace. It is recommended to equip computer system blocks containing EST software (here in afterreferred to as Electronic Signature Tools) with autopsy monitoring tools. You must only log in to your computer using authentication data (username/password). It is not recommended to use the computer administrator account to work with the DBO System.

15. Repair and / or subsequent use of system blocks should be carried out after removing the EST software from them or dismantling the information storage facilities.

16.In order to improve the security of electronic payments in the DBO System, prevent unauthorized access from other workplaces and counteract fraudulent actions in relation to funds in the Client's accounts, the Bank strongly recommends using the free filtering service provided by it for IP addresses and MAC addresses of the Client's computers from which work is performed in the RBS System. For this purpose, the Bank recommends that Customers who work on a dedicated Internet channel from static IP addresses agree on their list, exclusively from which the Client will be allowed to work in the RBS System. All other IP addresses that are not included in the list of allowed ones will be banned from using the Client's RBS System. When connecting, Clients must fill out and send to the Bank in writing, signed by the head of the organization with a seal certifying it, an Application for restricting work in the RBS System from certain addresses (Appendix No. 9 to the Terms and Conditions). This service is provided in accordance with the Letter of the Bank of Russia dated 30.01.2009 No. 11-T "On recommendations for Credit institutions on additional information security measures when using Internet Banking systems".

17. The Bank informs all its Customers that it does not send out e-mails (and also does not apply by phone) with a request to send the Item Instance Key and password, and does not send out any programs by e-mail. Any letters of such content sent on behalf of the Bank's employees are falsifications. After receiving them, you should contact the bank's personal manager or technical support officer, as well as convey the information to your direct supervisor.

18. The Bank reminds you that the entire responsibility for the confidentiality of the Client's EP Keys, as well as for the EPD with the correct Client's EP lies entirely with the Client, as the sole owner of the EP Keys.

19. In case of Compromise of the EP Keys, the Client is obliged to take all measures to stop any actions in the RBS System, as well as immediately verbally via telephone communication by phone (495)-287-30-99 upon presentation of the Code Word, inform the technical support service of the Bank's RBS System about this fact.

20. Upon the fact of compromising the E-mail Address Keys, the Client must submit a written application to the Bank in person or by e-mail about blocking their work in the DBO System, as well as organize an internal investigation, the results of which are reflected in the internal investigation report.

21.In order to avoid compromising the Item Instance Keys, it is recommended to lock the computer during short breaks in work, as well as at the end of the working day; resume computer activity using the access password. It is recommended to remove the key information carrier from the storage locations only when it is directly presented to the computer for installing the item instance; it is recommended to store the key information carrier in a secure place for the rest of the time during the session of working in the DBO System.

22. It is not allowed to:

- attempt to write extraneous data and files to the key information storage medium.
- make attempts to remove a copy of the Item Instance Keys from the key information storage medium.
- disclose the contents of key information carriers or transfer the carriers themselves to persons who are not allowed to access them;
- display the contents of the Item Instance Keys on a display, printer, or other external information display devices.
- insert the key information carrier into the reader in modes that are not provided for by the standard mode of operation of the DBO System, as well as into readers of other computers that are not intended to work in the DBO System;
- leave key media unattended in your computer's readers or on your desk.

23. It is recommended to install licensed software, including antivirus software, on all computers used for working with the DBO System, keep up-to-date antivirus databases, and regularly install Windows OS updates.

24. Provide a trusted environment on a computer designed to work with the DBO System. For what:

- Allocate a computer(s) that will not be used by the Client for any other purpose other than to work in the DBO System.
- Install a firewall on the computer or on the corporate server that prohibits Internet access from this computer to other sites, with the exception of the Bank's information site, the operational site of the Bank's DBO System and (if necessary) the sites of other banks ' DBO Systems, as well as preventing attacks on this computer from the Internet and the local network, and also unauthorized access to it from the network.
- If it is necessary to connect this computer to the local network of the organization for exchange with accounting systems, for example, 1C, provide a secure and restricted connection of this computer to the network resource of the 1C database.
- Disable the ability to capture remote control via a terminal connection of computers used for working in the DBO System by blocking ports 3389/tcp (RDP Remote desktop) and 5900/tcp (VNC) on the Firewall and disabling the “Remote Assistant” service on these computers.
- It is strongly recommended not to use remote desktop connection programs for working with the RBS system, such as ANYDESK, TEAM VEWER, and so on. This may lead to a compromise of the used item instance.
- Disable "Guest Access" by blocking the local Guest account on the computer running in the DBO System, and also do not use an administrative account when working normally.

- Enable Windows security logging in the operating system, install a licensed antivirus, and regularly update your antivirus databases to keep them up-to-date.
- Have a backup computer from which you can quickly log in to the DBO System in the event of a virus or other attack on the main computer.
- Do not use the premises of an Internet cafe or other guest places with Internet access as temporary workstations of the DBO System.

25. It is recommended to perform an additional control login to the DBO System on a regular basis (several times a day) to check the status of your current accounts on statements and track outgoing EPDs for the current day.

26. If it is not possible to log in to the DBO System or suspicious EPDs are detected that have not been created by the Client, you must immediately inform the Bank of this fact verbally by telephone (phone (495) 287-30-99) with the presentation of the Code Word.

In this case, the Bank will block EPDs that are in the "Processing" status until the circumstances are clarified.

27. Upon blocking the entrance to the RBS System and suspicious EDS, the Client must also personally report to the Bank, submitting a written application for blocking and/or revoking the suspicious payment and receiving a paper statement of accounts.

28. Some characteristic features of a hacker attack on the computer of a Client involved in working with the DBO System are:

- The site of the Bank's DBO System looks unusual, or the browser's address bar contains a link to a different site than the site of the Bank's DBO System. However, the browser returns an error for the site's security certificate.
- Inability to log in to the DBO System again with a password known to the Client (if there are no other reasons for blocking it).
- The key media does not contain a container with EP files, or the media is suddenly damaged/corrupted.
- In Windows OS, the antivirus detects a virus/Trojan, etc., or the antivirus returns an error and does not start.
- Unusual and uncharacteristic behavior of the computer (spontaneous reboots, especially in combination with the inability to continue normal booting, frequent freezes for a short period of time, including the so-called "blue screen of death").

29. In all the above cases, the Client should immediately stop trying to use this computer to work with the DBO System, do not try to fix the computer malfunction or cure the virus on their own, and apply to the Bank with oral and written statements about blocking work in the DBO System until all the circumstances are clarified and the reasons that led to damage to the computer and/or key media type.