

INFORMATION SECURITY MEASURES

1. Use only licensed software on the Workplace.
2. Use antivirus protection software in the Workplace and update it regularly; use licensed antispyware software and firewalls.
3. Do not reproduce or use the System/Online Banking System «KREDOBANK» and its documentation for purposes other than those specified in the Terms.
4. Ensure the secure storage of the information carrier with an Advanced Electronic Signature for the System ("Advanced ES for the System")/ Advanced Electronic Signature with a Qualified Certificate ("Advanced ES with a Qualified Certificate") / Qualified Electronic Signature ("Qualified ES"). Store the information carrier with an Advanced ES for the System/Advanced ES with a Qualified Certificate/Qualified ES in conditions that ensure its protection from unauthorized access by third parties, and ensure that access to the information carrier with an Advanced ES for the System/Enhanced ES with a Qualified Certificate/Qualified ES is granted exclusively to Users and only while working with the System/«KREDOBANK» Online Banking System. Do not allow Users to transfer information carriers with an Advanced ES for the System/Advanced ES with a Qualified Certificate/Qualified ES to other persons. The information carrier with an Advanced ES for the System/Advanced ES with a Qualified Certificate/Qualified ES shall be accessible only to the User. The method of storing the information carrier with an Advanced ES for the System/Advanced ES with a Qualified Certificate/Qualified ES shall prevent access by any other persons. The method of storing information carriers with an Advanced ES for the System shall ensure that they are accessible to the User only during their use while working with the System/«KREDOBANK» Online Banking System.
5. Ensure the One-Time Code is stored in a way that prevents its use by anyone other than the User for whom the One-Time Code was sent, and in the case of using a Mobile Authenticator – ensure that the Mobile Authenticator cannot be used by anyone other than the User.
6. Ensure restricted access to the Workplace where the System module/«KREDOBANK» Online Banking System is installed, or from which access to the System/«KREDOBANK» Online Banking System is performed, exclusively to properly authorized Users.
7. Ensure the confidentiality of data used for User authentication in the System/«KREDOBANK» Online Banking System (logins, passwords, One-Time Codes, etc.), including confidential information about Personal Work Keys (passwords, etc.), from any other persons.
8. Do not store Personal Work Keys, including their passwords, on the hard drive of the Workplace.
9. Store Personal Work Keys exclusively on portable information carriers (USB flash drives, CDs, etc.).
10. Do not use the System/«KREDOBANK» Online Banking System from Workplaces in public places (Internet cafés, libraries, etc.), or from any other equipment the configuration and operation of which are beyond the Client's control.
11. Ensure regular changes of passwords for Personal Work Keys.
12. Do not use simple passwords for Personal Work Keys (simple passwords include, in particular: the User's first or last name, date of birth, repeating identical characters, using characters sequentially arranged on the keyboard, etc.). The password shall be changed regularly and shall consist of at least 8 (eight) characters (numbers, letters, etc.).
13. To access the System's web page, use only the following address: <https://ifobs.kredobank.com.ua>.
14. To download and install the appropriate mobile application of the System/«KREDOBANK» Online Banking System/Mobile Authenticator on a mobile device, use only official app stores (if the device runs on iOS, the System/«KREDOBANK» Online Banking System mobile app shall be downloaded from the App Store; if the device runs on Android, the System mobile app shall be downloaded from the Play Market).
15. Restrict access to the Workplace for unauthorized persons.
16. Ensure that the Advanced ES for the System/Advanced ES with a Qualified Certificate/Qualified ES is available at the Workplace only during the User's work with the System/«KREDOBANK» Online Banking System.
17. If unusual behavior of the System/«KREDOBANK» Online Banking System or any changes in its interface are detected, immediately contact the Contact Center to determine whether such changes are related to a software update of the System/«KREDOBANK» Online Banking System.
18. If you suspect the occurrence of Unauthorized Funds Withdrawal/ Unauthorized Access, immediately notify the Bank by contacting the Contact Center.
19. Use the SMS notification service about account transactions as an operational tool to monitor fund movements.
20. Do not provide anyone with confidential data used to access the System/«KREDOBANK» Online Banking System, as the Bank never sends emails, SMS, or other messages requesting confirmation or submission of Client (User) confidential data; such messages are fraudulent (phishing).
21. Ensure the mobile phone screen is unlocked using a password/FaceID/TouchID.
22. Use different PIN codes and passwords for the mobile device and applications, including online banking mobile applications.
23. Do not install applications obtained from unknown sources or applications the operation of which you do not understand, or those requiring a large number of additional installations.

24. When installing applications on a mobile device, check what permissions the application requests (remote device control, etc.) and do not install applications that request permissions which may allow other persons to use the mobile device and/or obtain confidential data used to access the System/«KREDOBANK» Online Banking System.
25. Install available operating system and application updates on your mobile device in a timely manner when it is used to connect the User to the System/«KREDOBANK» Online Banking System.
26. If there are suspicions that the phone is infected with viruses, do not enter sensitive information (logins, passwords, etc.) until it has been checked with licensed antivirus software and/or you have sought assistance from specialists.
27. In case of loss of a mobile device or SIM card malfunction, contact your mobile operator and, if necessary, the Bank. Notify the Bank and temporarily restrict access to the System/Online Banking System and your mobile operator's personal account until the situation is clarified and access is restored.
28. Comply with other information security measures specified in the Terms and those published on the Bank's website.

Attention!

The Bank never, under any circumstances, sends emails, SMS messages, or other communications requesting you to confirm or provide your confidential information (including Personal Work Keys, login, password, or One-Time Password). Such messages are fraudulent (phishing).

BANK:

CLIENT:

(Full name of the Bank's representative, signature)

(Full name of the Head, signature)

(Full name of the Chief Accountant, signature)

L.S.

L.S.
