

PUBLIC OFFER
of the "KSB Commercial Bank " Closed Joint Stock Company
(for a conclusion of an Agreement for the provision of banking services through the
"Internet/Mobile Banking" system (for individuals))

_____ 20 _____

City of _____

1. GENERAL TERMS AND CONDITIONS

- 1.1. This document is an official offer (public offer) of the "KSB Commercial Bank" Closed Joint Stock Company (hereinafter referred to as the Bank) addressed to interested individuals to conclude, in accordance with Article 398 of the Civil Code of the Kyrgyz Republic, an Agreement for the provision of banking services through the Internet / Mobile Banking system, published on the official website of the Bank at www.ksbc.kg, under the terms and conditions below.
- 1.2. The Agreement for the provision of banking services through the Internet / Mobile Banking system of the " KSB Commercial Bank " Closed Joint Stock Company (hereinafter referred to as the Agreement) is concluded in a special manner: by acceptance to this offer without signing by the parties. This offer has legal force in accordance with Article 402 of the Civil Code of the Kyrgyz Republic and is equivalent to the Agreement signed by the parties. The text of the Agreement is also given in this offer.
- 1.3. Acceptance to this offer, as well as full and unconditional acceptance of the conditions set out below, is considered to be the signing of the relevant clause in the Appendix for connection to the Internet/Mobile-Banking system for individuals. If the customer disagrees with any clause of this offer, it is proposed to conclude an agreement with the Bank in writing.

2. SUBJECT OF THE CONTRACT

- 2.1. The subject of this Contract is the provision of remote banking services to the Customer through the Internet/Mobile Banking system, which ensures the Customer's work with the Bank through the WEB Application and the Internet in accordance with the current tariffs of the Bank at the time of the provision of the service, through the official link <https://ibank.ksbc.kg> on the terms provided for by this Contract and the Bank Account Contract and / or the Contract on the Issuance and Maintenance of a Bank Payment Card of an Individual, concluded between the Customer and the Bank.
- 2.2. The list of banking services provided to the Customer in accordance with this Contract includes the following:
 - acceptance of payment documents (orders) in national and foreign currencies;
 - acceptance of payment documents (orders/applications) for conversion; (purchase/sale) of foreign currency;
 - provision of account statements;
 - provision of information on exchange rates and financial reference information;
 - provision of payment orders for instant payments.
- 2.3. The Customer acknowledges that the receipt by the Bank of electronic payment documents is legally equivalent to the receipt of payment documents on paper, certified by signatures in accordance with the signature samples provided to the Bank. The Customer entitles the Bank to use electronic payment documents on an equal footing with payment documents on paper, certified by signatures, in accordance with the Customer's sample signatures provided to the Bank.

- 2.4. The Customer obtains the right to remote banking services through the Internet/Mobile Banking system after the conclusion of this Contract, the mandatory indication of the mobile phone number and e-mail address.
- 2.5. The Bank is the owner of the Internet/Mobile Banking system in terms of the technical means it operates, as well as the software and information resources of the System hosted on the technical means of the Bank.
- 2.6. The Customer bears all the risks associated with connecting his technical means to the Internet, independently ensures the protection of his own technical means and bears the risks resulting from unauthorized access, password cracking, fraudulent, hacker, virus attacks from the Internet.
- 2.7. The Parties acknowledge as a single time scale when working with the Internet/Mobile Banking system the Bishkek time stamped by the System in electronic documents.

3. RIGHTS AND OBLIGATIONS OF THE BANK

- 3.1. The Bank is obliged:
 - to issue a pin-envelope with unique access codes to the Internet/Mobile Banking system at the request of the Customer in accordance with Appendix 1;
 - to provide a full consultation to the Customer on working with the Internet/Mobile Banking system;
 - to keep secret regarding the terms of this Contract, keep secret about the Customer's operations and provide information on them to third parties only in cases stipulated by the legislation of the Kyrgyz Republic.
- 3.2. The Bank accepts electronic payment documents from the Customer around the clock (including non-working and holidays). Execution of the received electronic payment documents of the Customer is carried out by the Bank in accordance with clause 3.4. of this Contract.
- 3.3. Electronic payment documents are accepted by the Bank for execution only when issued in accordance with paragraphs. 4.5-4.6 of this Contract and the availability of the Customer's electronic signature.
- 3.4. The execution of the Customer's payment documents is carried out by the Bank on business days during the Bank's business day from 9:00 to 17:30 Bishkek time. Payment documents received by the Bank before 11:45 am are processed on the same transaction day, and documents received after 11:45 am, at the request of the Customer, are processed on the same transaction day using the gross system with payment at the current rates of the Bank or on the next transaction day.
- 3.5. The Bank immediately stops accepting the Customer's electronic payment documents and informs him within an hour if there is a suspicion of a threat of unauthorized access to his bank accounts, as well as in the event of receiving a corresponding notification from the Customer, until the circumstances of the incident are clarified. The threat of unauthorized access is the appearance of a damaged electronic payment document.
- 3.6. The Bank, at the written request of the Customer, re-issues access codes to improve the security of the electronic payment system.
- 3.7. In the event of a discrepancy between the balances on the Customer's bank account between the hard copy statement provided by the Bank and the electronic statement, the hard copy statement shall be considered correct. To correct the electronic statement, you must send an official letter to the Bank.
- 3.8. In case of incorrect indication of the details of the payment document (payment purpose code, purpose of payment, account number, etc.), the Bank returns the payment document without execution.
- 3.9. In case of technical problems in the process of using the Internet/Mobile Banking system, make the necessary efforts and take all possible actions to eliminate them within a reasonable

time. At the same time, the Customer is not entitled to make claims to the Bank, and during the period of elimination of technical problems, he must carry out banking operations in the usual way using paper media.

- 3.10. Immediately block access to the Customer's account upon receipt of a relevant request from the Customer, in the manner prescribed by this Contract.
- 3.11. Provide the Customer with new access codes to the Internet/Mobile Banking system at the request of the Customer. **The Bank has the right:**
 - 3.11.1. to unilaterally change the Bank's tariffs for servicing the Internet / Mobile Banking system, with the obligatory notification of the Customer, by posting new tariffs on the Bank's official website, on information stands in the Bank's operating room and via SMS messages to the customer's mobile phone number, provided that these changes do not worsen and / or infringe on the rights and legitimate interests of the Customer;
 - 3.11.2. to make direct (without the consent or payment order of the Customer) debit from any of the Customer's accounts the amounts of the Bank's remuneration for the services provided, commissions for transactions performed in the Internet / Mobile Banking system, as well as write-offs of erroneously credited amounts, in cases where the fact of erroneous crediting of funds is established to the Customer's accounts, the amounts of any debt of the Customer to the Bank for any obligations, as well as in other cases established by the legislation of the Kyrgyz Republic;
 - 3.11.3. to refuse the Customer to perform a transaction in the System in case of incomplete (incorrect) indication by the Customer of the details of the transaction being performed, inconsistency of the transaction being performed with the current legislation of the Kyrgyz Republic, as well as in cases of insufficient funds on the Customer's account to complete the transaction and / or to pay the Bank's remuneration for the transaction operation;
 - 3.11.4. to limit, and in exceptional cases deny access to the Customer in case of failure of the Bank's software, as well as in the event of any adverse consequences of unauthorized access to the System; In order to prevent unauthorized access to the Internet/Mobile Banking system, if an incorrect password is entered more than 3 (three) times, the security system blocks the user's account (account), in order to unlock access to the account, the customer undertakes to contact the Bank's employees at a personal meeting face of tellers with the provision of the necessary documents confirming his identity;
 - 3.11.5. to carry out a temporary shutdown of the System to carry out the procedure for changing the software and carrying out preventive maintenance;
 - 3.11.6. in case of closure of the Customer's account(s), to immediately cancel the Customer's access to the System.

4. RIGHTS AND OBLIGATIONS OF THE CUSTOMER

- 4.1. To work in the "Internet-Banking" system, the Customer uses any personal computer with the ability to access the global Internet. To work in the "Mobile Banking" system, the Customer uses any mobile phone based on the Android operating system (version 4.0 or higher) or iPhone (version 12.0 or higher), a series of smartphones developed by Apple, running the iOS operating system, with the ability to exit to the global Internet.
- 4.2. The Customer undertakes to keep secrecy regarding the terms of this Contract and comply with all requirements of the Bank in connection with remote banking services, keep the rules and access codes to the Internet Banking system secret from third parties, and immediately, by any available means, inform Bank about the occurrence of a threat of unauthorized access to the Internet/Mobile Banking system in the following cases:
 - disclosure of the password or suspicion of its copying by third parties;
 - any personnel changes within the Customer's organization affecting persons associated with the Internet/Mobile Banking system.
- 4.3. The Customer undertakes to change the initial access codes and keep the username, password and PIN code secret from third parties for accessing the Internet account
- 4.4. Periodically, but not less than once every three months, change the password for access to the Internet/Mobile Banking system.
- 4.5. Periodically check the correspondence of bank details and payment details in the payment directories, check the compliance of these details with the bank details of the recipients of transfers.
- 4.6. The Customer undertakes to fill out electronic payment documents in accordance with the legislation of the Kyrgyz Republic and the requirements of the Internet/Mobile Banking system, be fully financially responsible for all transactions made by the Customer in the Internet/Mobile Banking System, comply with the legislation on combating the financing of terrorist activities and legalization (laundering) of criminal proceeds, as well as, at the request of the Bank, provide the documents requested by the Bank, on the basis of which the operation (transaction) is performed.
- 4.7. The Customer undertakes to use the Internet/Mobile Banking system only on technically sound and safe equipment.
- 4.8. The Customer does not have the right to duplicate electronic payment documents. Documents that simultaneously have the same number, amount, date, sender's account and recipient's account, bank identification code (BIC) are considered duplicate documents.
- 4.9. In case of sending duplicate electronic payment documents to the Bank having the same numbers due to the fault of the Customer, the Customer must notify the Bank in writing or by calling the Bank's public number on the same business day.
- 4.10. The Customer undertakes to timely pay for the Bank's remote banking services under this Contract in accordance with the Bank's Tariffs.
- 4.11. **The Customer has the right:**
 - 4.11.1. to use the full range of services of the "Internet/Mobile Banking" system on the terms stipulated by this Contract;
 - 4.11.2. to change the original access codes, password and PIN for accessing the Internet account. Password requirements must meet the following criteria:
 - at least 8 characters;
 - at least one uppercase and one lowercase letter;
 - only Latin letters;
 - at least one digit;
 - without spaces;
 - Other valid characters: ~! ? @ # \$ % ^ & * _ - + () [] { } > < / \ | " ' . , ;
 - If you change or reset your password, your new password must be different from the previous one.;

4.11.3. to receive confirmation from the Bank on paper of the execution of a payment order for banking transactions made through the Internet/Mobile Banking systems.

5. PAYMENT UNDER THE CONTRACT

- 5.1. The Customer pays commissions for connection and maintenance of the system in accordance with the current Tariffs of the Bank, posted on the official website of the Bank (www.kxbc.kg), on information stands in the Bank's operating room.
- 5.2. The fee for the services provided by the Bank at the request of the Customer, specified in clause 1.2, is charged separately according to the current tariffs of the Bank.
- 5.3. The Bank may revise the current tariffs for servicing the Internet/Mobile Banking system.

6. LIABILITY OF THE PARTIES

- 6.1. The Parties are responsible for disclosing the content of this Contract and the obligations arising from it.
- 6.2. The Bank is responsible to the Customer for the safety of money, the correctness and timeliness of the execution of the Customer's instructions in accordance with the Bank Account Contract / Bank Account Contract and / or the Contract on the Issuance and Maintenance of a Bank Payment Card No. _____ dated ____ _____ 20__ of an Individual, under which this Contract is concluded, and the legislation of the Kyrgyz Republic.
- 6.3. The Customer is responsible for the correctness of filling in the data contained in the Customer's electronic payment documents.
- 6.4. The Bank is not responsible for debiting funds from the Customer's bank account on duplicate payment documents (in electronic form or on paper) if the Bank was not notified in a timely manner about sending duplicate payment documents. The bank is not responsible:
 - for errors, delays or inability of the Customer to gain access to the Internet/Mobile Banking system related to a malfunction of the Customer's equipment and/or communication failures in communication channels;
 - for damage to the Customer's equipment or information stored in the Customer's equipment, for the safety of the Customer's software and personal computer from various viruses and other damage;
 - for failure to comply with the Customer's instructions using the Internet/Mobile Banking system, if the Customer's account was seized or operations on it were suspended by the Customer in the manner prescribed by this Contract and / or in accordance with the legislation of the Kyrgyz Republic;
 - for means, products and services, with the help of which services are provided in the Internet/Mobile Banking system, provided by a third party (Internet access provider, etc.);
 - for damage caused to the Customer as a result of unauthorized access to the system located on the Bank's web server by third parties, in cases where such access occurred in a situation that is not subject to or not subject to control by the Bank (compromised logins and passwords of the Customer);
 - for the transfer of unblocked mobile devices with an open application to the Internet/Mobile Banking system to third parties;
 - for non-execution of the Customer's payment orders in the System, if the order was not provided in full (incorrect) format and/or included information that contradicts the current legislation of the Kyrgyz Republic;

- for a delay in payment due to the fault of third parties (other banks), including if the delay occurred due to a difference in the working hours of the Bank and the correspondent bank and/or another bank, due to holidays in the country of the correspondent bank, as well as in other cases that occurred through no fault of the Bank;
- for damage caused to the Customer as a result of fraudulent, hacker, virus attacks from the Internet;
- for failure to comply with the Customer's instructions using the System, if the Customer's account was seized or operations on it were suspended in accordance with the current legislation of the Kyrgyz Republic;
- for the consequences of the Customer's untimely notification of the Bank about the loss (theft) of the password and/or username and/or PIN code, about incorrect transactions and attempts of unauthorized access to the Customer's account using the Internet/Mobile Banking system (or about committing access attempts). Any loss or liability resulting from such or similar actions shall be borne by the Customer.

7. CIRCUMSTANCES OF INSUPERABLE FORCE (FORCE MAJEURE)

- 7.1. The Parties are released from liability for non-fulfillment or improper fulfillment of obligations under the Contract, if the non-fulfillment or improper fulfillment was the result of force majeure circumstances (force majeure).
- 7.2. By force majeure, the Parties understand the circumstances that arose after the signing of the Contract as a result of unforeseen and inevitable events of an emergency nature, such as: war and hostilities, power outages, software failures, natural or other disasters occurring in areas officially recognized as such, actions of the legislative and / or executive authorities of the Kyrgyz Republic, the National Bank of the Kyrgyz Republic prohibiting or restricting activities directly related to the subject of this Contract.
- 7.3. The Party, for which it became impossible to fulfill obligations under the Contract due to the circumstances specified in clause 6.2, must notify the other Party in writing of the occurrence and termination of these circumstances without delay and, upon request, provide the opposite Party with evidence confirming the occurrence and / or termination of force majeure circumstances. Evidence of the occurrence and duration of these circumstances are written documents issued by the competent authorities.
- 7.4. In the cases provided for in paragraphs 6.1.-6.3. the deadline for fulfilling obligations under the Contract is extended in proportion to the time during which such circumstances and their consequences are in effect.

8. SPECIAL TERMS OF THE CONTRACT

- 8.1. The Contract is subject to revision in case of changes in the legislation of the Kyrgyz Republic and the requirements of the National Bank of the Kyrgyz Republic in terms of relations stipulated by this Contract.
- 8.2. From the moment of signing this Contract, the agreements concluded between the Bank and the Customer for settlement and cash services of the Customer's accounts do not lose their legal force.
- 8.3. The conditions for the provision of additional services in the Mobile Banking system that are not specified in this Contract must be specified in an additional agreement signed by both parties and which is an integral part of this Contract.
- 8.4. The Customer hereby confirms that prior to the signing of this Contract, he has read and agrees with all the terms of use of the Internet/Mobile Banking and tariffs for the services provided by the Bank.

9. DISPUTE RESOLUTION

- 9.1. Disputes under this Contract shall be resolved by the Parties through negotiations, taking into account mutual interests. In the absence of the consent of the Parties on controversial issues within 10 working days from the date of the dispute, disputes under this Contract are considered by the judicial authorities of the Kyrgyz Republic in accordance with the legislation of the Kyrgyz Republic.
- 9.2. In all other respects not stipulated by this Contract, the Parties are guided by the legislation of the Kyrgyz Republic.
- 9.3. The requirement to block access to the System received by the Bank in the manner specified in clause .10. of this Contract is considered to come from the Customer and claims for the consequences of blocking by the Bank are not accepted, to which the Customer, by signing this Contract, expresses his unconditional consent.

10. VALIDITY OF THE CONTRACT

- 10.1. The Contract comes into force from the moment of its signing by both Parties and is valid until it is terminated at the initiative of either Party.
- 10.2. Termination of the Contract occurs subject to the completion of mutual settlements in the following cases:
 - closure for any reason of a bank account, transactions on which were carried out using the Internet/Mobile Banking system,
 - by mutual decision of the Parties;
 - unilaterally, with prior written notice to the other Party at least 10 (ten) calendar days before the expected date of termination.
- 9.3. All changes and / or additions and annexes to this Contract must be made in writing and signed by authorized representatives of both Parties and are integral parts of the Contract.
- 9.4. This Contract is made in two copies in Russian, having the same legal force, one copy for each Party.

MEMO
on information security when working with the service "Internet/Mobile Banking"

The security of using remote banking services (hereinafter referred to as RBS) consists of the totality of all security requirements when working with RBS and depends on their compliance by the Customer.

Follow simple recommendations for working with RBS, this will allow you to avoid unauthorized access to your data by third parties.

Requirements for the password of a personal workstation - a computer connected to RBS:

- Never write down your computer login and password in places accessible to third parties, but rather just remember them.
- Create your password using uppercase and lowercase letters and numbers, do not use easy-to-guess passwords such as QWERTY, 12345678, etc.
- Change your password periodically. If you suspect that someone has information about your username and password, be sure to change your password.
- Never share your login and password information with anyone, including the Bank's employees.
- Do not leave a computer turned on with an open RBS web page unattended - you must leave the site where electronic transactions are carried out, even if the computer is left unattended for a short time.
- Avoid using other people's computers for electronic transactions.

Computer software requirements:

- Use strictly licensed software installed or planned to be installed on your computer.
- Keep your computer's operating system and computer application software up-to-date using automatic updates or only from trusted sources that guarantee no malware. Keep in mind that when using non-updated or old versions of software, unpatched bugs in the software will be used by attackers to take control of your computer.
- Use and promptly update licensed specialized information protection software - anti-virus programs, personal firewalls, anti-tampering tools, etc. Remember that malicious software (computer viruses, Trojans, etc.) is often used the ability to send sensitive data or allow attackers to remotely control a computer.
- Before carrying out any online transactions or providing personal information, you must ensure that the correct RBS web page is being used. The address of the official address of the RBS Bank is <https://ibank.ksbc.kg>. It is necessary to beware of fake web pages created for the purpose of scams. Avoid redirecting or linking to other untrustworthy pages. Do not save the RBS access password directly in the computer browser.
- Check your transaction history and statements regularly to track down errors or unauthorized account transactions. Immediately inform the Bank of any cases of unauthorized use of the account or transactions.

Requirements for restricting access to a computer, logins, passwords and private key carriers:

- Strictly observe the rules of limited access to the computer. Remember that any physical access to a computer is a potential opportunity to install a malicious program on the computer (via removable media or by accessing a malicious Internet resource), with the possibility of its subsequent use by attackers to steal money through remote banking.
- Comply with the rules of access to the storage of secret keys (only trusted persons of the customer should work with the key storage and the computer).
- Connect the media with the Electronic Signature key to the computer only for the duration of communication sessions with the bank, and after they are completed, you must immediately disconnect the media from the PC and put it in a storage location (safe) inaccessible to unauthorized persons. Key safety is the main factor in ensuring information security when working with the RBS system.

General Recommendations:

- Never open suspicious files sent to you by email.
- Do not respond to suspicious e-mails or phone calls asking you to provide the RBS login, any passwords, Code word and your other confidential data (Bank employees will never, under any circumstances, ask you for such information).
- Immediately inform the Bank about emergency situations and suspicions of violation of computer security (infection of the computer with viruses, unauthorized access to the RBS workplace, compromise of the signature key).