



Rules for provision and use of “KICB”/ “KICB BUSINESS” internet-banking system in CJSC “Kyrgyz Investment and Credit Bank”

1. Terms and definitions

Bank – CJSC "Kyrgyz Investment and Credit Bank".

Client - an individual/individual entrepreneur/legal entity, connected to the “KICB”/ “KICB BUSINESS” internet-banking system in accordance with these Rules.

Account - any bank account opened for the Client on the basis of an agreement concluded between the Bank and the Client.

Remote banking system “KICB”/ “KICB BUSINESS” - (hereinafter referred to as the "KICB" system) - a set of services for remote access and management of the Client's bank accounts using a computer, mobile phone or other device with Internet access. It includes the following services:

- Internet banking - a remote service channel provided to the Client through a web-browser;
- Mobile banking - a remote service channel provided to the Client through a mobile application.

Remote banking service - when the Bank provides the Client with opportunity to carry out banking operations without need to come to the Bank, using “KICB”.

Personal Account is a website section that allows the user to get access to their bank accounts and remotely manage their bank accounts.

Authorization data - login, password, One Time Password, PIN code and biometric data of the Client, used by the Bank to authenticate him/her when entering “KICB” system.

Client Authentication is the establishment of the Client's authenticity by verifying the authenticity of submitted identifier (login, password, biometrics, pin code, etc.) based on the Authorization data.

Login - a unique electronic name/identifier used to authenticate the Client in “KICB” system. When the Client connects to “KICB” system, the login is initially generated by the Bank, later the login can be changed by the Client independently.

Password - a unique sequence of characters intended for the Client's authentication in “KICB” system.

One Time Password (hereinafter referred to as the OTP code) is a one-time password for Client authentication or authorization of transactions sent to the Client's mobile phone via SMS or generated by the Google Authenticator mobile application, or generated by a token.

PIN code - a unique sequence of characters used to authenticate the Client in the mobile application. After the first successful authentication of the Client, the PIN code shall replace the login and password (if there is no password or biometrics on the hardware device).

Biometric data - the function of the Client's fingerprint or Client's face recognition, read and processed by the mobile phone and used to authenticate the Client. It is an optional replacement for the pin code and is available if the Client's mobile phone supports such functionality.

Google Authenticator is a mobile application installed on the Client's mobile phone that generates an OTP code.

Token is a physical device that generates an OTP code.

Push notification is a message sent by the Bank via the Internet to the Client's mobile device with a mobile application installed on it.

Tariffs - the rate of payment established and charged by the Bank for the services provided. The current Tariffs are communicated to the Client by posting information on the website www.kicb.net.

Application - the Customer's application for servicing in the “KICB” system submitted to the Bank, signed by the Customer in the form approved by the Bank.

Operation - any banking operation carried out by the Bank at the Client's request.

Client's Order is an electronic payment document, which contains the Client's instructions to the Bank to carry out banking operations stipulated by these Rules and the functionality of the “KICB” system.

Authorized work session - the period of the Client's work in the “KICB” system, beginning of which is the execution of the Client's Authentication procedures. The end of an authorized session of the Client's work in the “KICB” system is the moment of log-out from it.

An authorized person is a person authorized by the Client in accordance with the procedure established by the legislation, who is entitled to manage the Client's accounts, funds on these accounts on behalf and at the expense of the Client, perform operations on the Client's account, to receive information about the balances on the Client's accounts, and receive statements about cash flow through the Client's accounts.

Confidential Information - any information (data) received, transmitted and used by the Bank, the Client or an Authorized Person during use of remote banking services, including Authorization data and information constituting a bank secret.

View mode - access to “KICB” system without possibility of performing transactions.

Full access mode - access to the “KICB” system with the ability to perform transactions.

Party - the Bank or the Client.

Parties - the Bank and the Client.

2. General Provisions

2.1. These Rules are a public offer - the Bank's offer to conclude an agreement for remote banking services using the “KICB” system based on terms specified in these Rules.

The contract for remote banking services using the “KICB” system shall be considered concluded and becomes effective from the moment the Client signs and submits the Application.

These Rules are an integral part of the Application, contain its main terms and conditions, and together constitute a single agreement for remote banking services using “KICB” system.

These Rules determine the procedure and conditions for the Bank to provide the Client with remote access to its Account via Internet using the “KICB” system, as well as regulate the relationship between the Client and the Bank arising under these Rules.

2.2. When the Client signs and submits the Application to the Bank, it means that he/she expresses his/her unconditional and full consent to accede to these Rules and to accept the terms and requirements of the Rules.

2.3. The Rules shall be binding on both by the Client and the Bank.

2.4. By signing the Application and submitting it to the Bank, the Client confirms that:

2.4.1. before submitting the Application to the Bank, the Client has fully read and agrees with these Rules and the Bank's Tariffs for the services provided, undertakes to pay for the Bank's services in accordance with their volume and applicable tariffs on the terms provided for by these Rules, undertakes to comply with the conditions and requirements of these Rules, undertakes to monitor and comply with changes in the Bank's Tariffs and these Rules on the Bank's website www.kicb.net;

2.4.2. The Client is familiar with and agrees that the Bank has the right to unilaterally amend or supplement these Rules, change or establish new Bank Rates with notifying the Client about this by posting electronic versions of new editions of the named documents on the Bank's website www.kicb.net 10 (ten) calendar days before the date of entry into force of these changes or additions, except for changes and additions due to the requirements of the legislation of the Kyrgyz Republic, for which an earlier date of entry into force is stipulated by the regulatory acts of the Kyrgyz Republic;

2.4.3. The Client is familiar with and undertakes to comply with the security requirements for the provision of remote banking services provided for by these Rules and the security recommendations posted in the “KICB” system.

2.5. The client who acceded to these Rules assumes all the rights and obligations provided for by these Rules, including all and any changes and additions made to them.

2.6. When the Client logs into the “KICB” system and before starting the service, the Client should familiarize himself with the current version of these Rules posted on the Bank's website www.kicb.net.

2.7. The Client, by connecting to the “KICB” system, agrees to banking services through the Internet, realizing that the Internet is not a secure communication channel and the Client, who acceded to these Rules, shall assume all risks:

2.7.1. arising from use of such a communication channel, including those related to the possible access of third parties to the Client's Authorization Data and performance by a third party, who became aware of the Client's Authorization Data, expenditure and other operations on the Client's Account (s) and other actions to manage the Client's account (-s);

2.7.2. connected with connection of its technical means to the Internet and independently ensures the protection of its own technical means from unauthorized access and malicious software;

2.7.3. and assumes all possible losses, damages, etc., arising from use of remote banking services through the Internet, including as a result of fraudulent, hacker, virus attacks from the Internet and hereby the Client guarantees that he/she will not make any claims against the Bank, will not file any claims against the Bank

in such cases, since the Bank has previously and fully informed the Client about the possible risks. The Client hereby acknowledges and confirms that he/she himself/herself is the initiator of providing him/her with the technical ability to manage the Account (s), manage funds on the Account (s) and make payments and Transactions using remote banking services, as well as that he releases the Bank from any liability, and the Bank, accordingly, does not bear any responsibility to it for any consequences that may arise for the Client in case of interception by third parties of control of the Client's personal computer, mobile phone, theft of Authorization data or the Client's failure to comply with security procedures.

2.8. The types and amount of fees payable by the Client when using the “KICB” system shall be determined by the Bank's Tariffs. The Client undertakes to pay for remote banking services in accordance with the Bank's Tariffs on the terms determined by these Rules.

2.9. The Client has the right to refuse to use the “KICB” system by submitting an appropriate application to the Bank, provided that there are no disputed Operations, arrears in payment for the services of the Bank and third banks participating in the Client's Operations, other unfulfilled obligations to the Bank and any other claims of the Bank, connected with remote banking services of the Client and his/her Accounts.

2.10. Requests for blocking the access to the “KICB” system received by the Bank in the manner prescribed by these Rules are recognized by the Parties as originating from the Client and claims for the consequences of blocking by the Bank are not accepted, to which the Client expresses his/her unconditional consent.

3. The procedure for provision access and use of “KICB” system

3.1. The Bank shall provide the Client with access to “KICB” system on the basis of the Client's written Application, which can be submitted by him/her, both at the time of concluding the "Agreement for opening and maintaining a bank account in national and foreign currencies" or "Agreement for accession of the Cardholder", so and at any other time during the validity period of these Agreements.

3.2. The right to use “KICB” system shall be granted by the Bank only to the Client personally or to the Client's Authorized Persons.

3.3. Initially, the Password shall be generated by the Bank when connecting to “KICB” system, after successful Authentication, the Client can change the Password an unlimited number of times at his/her own discretion, subject to the requirements for passwords.

3.4. OTP code can be sent to the Client to the mobile phone via SMS or it can be generated via the Google Authenticator mobile application or Token.

3.5. The method of obtaining OTP-code shall be chosen by the Client at the time of submitting the Application to the Bank, subsequently it can be changed at the Client's request.

3.6. The Client's access to the “KICB” system shall be carried out through the Internet by means of a web browser and a mobile application. It is mandatory to use the most current versions of web browsers. The application is supported only by the following mobile operating systems: iOS and Android.

3.7. All Operations made through “KICB” system within the Authorized Session of Work are unconditionally and unconditionally recognized by the Parties as Operations performed personally by the Client or his/her Authorized Person, and the Client bears full financial responsibility for such Operations.

3.8. All transactions in “KICB” system, both to obtain information and to perform Operations, performed within the Authorized session of work, are unconditionally recognized by the Parties, performed personally by the Client or his/her Authorized Person, and the Client shall be bear a full financial responsibility for such Operations ...

3.9. The Client shall be obliged to treat the performance of Transactions through “KICB” system with due caution, as well as to take reasonable measures to reduce the likelihood of performing unintentional or accidental Transactions. All Transactions performed during the authorized work session, including payment for the goods/services, transfers and payments shall be considered executed by the Client's order and confirmed by him/her.

4. Main requirements on observation of security and confidentiality

4.1. This section shall define the rules mandatory for the Client to comply with in order to ensure the required level of security when using “KICB” system, and also includes a list of measures to ensure the confidentiality of client data and the Operations performed by the Client.

4.2. The Bank carries out, and the Client acknowledges the Bank's right to save in the Bank's database all events and actions performed within the framework of the authorized work session.

4.3. On the part of the Bank, information security requirements when using “KICB” system by the Client shall be ensured by taking the following measures:

- 4.3.1. obligatory assignment of a unique login to each Client;
- 4.3.2. mandatory generation of the Password in ways that exclude the possibility of access to information about the Password for any third parties;
- 4.3.3. to set the requirements for password complexity;
- 4.3.4. to limit the number of attempts to enter the Password in case of its incorrectness;
- 4.3.5. to limit the number of attempts to enter PIN code if it is incorrect;
- 4.3.6. mandatory entry of OTP code when performing certain types of operations, as well as in case of authentication in the web-version;
- 4.3.7. to use the Client's Biometric Data as Authorization Data for a mobile application, if such functionality is supported by the Client's device;
- 4.3.8. to set the time limit for the validity of the OTP code;
- 4.3.9. there will be a failure of the mobile application of the “KICB” system on the Client's mobile device (mobile phone and/ or other device that allows the use of the Bank's application) when the application of the “KICB” system on the device determines the rights of full access to the operating system and all functions of the mobile device, which entailed the removal of restrictions by the manufacturer or telecom operator for manipulating system applications and provided ability to run applications that require administrator rights (root and/ or jailbreak);
- 4.3.10. other methods established by the Bank as ways to increase the level of information security of “KICB” system.

4.4. The Client shall mandatory execute the following measures to ensure information security when the Client uses “KICB” system:

- 4.4.1. The client must be sure to keep the Login, Password, OTP-code, PIN-code confidential. It is strictly prohibited to transfer the Authorization Data to third parties both in oral or in written form;
- 4.4.2. The Client should change the Password on a regular basis;
- 4.4.3. If the Client has the slightest suspicion or revealed facts that indicate:
 - *access of third parties to the Client's Authorization Data;*
 - *access of third parties to the “KICB” system on behalf of the Client;*
 - *the loss (theft) of a mobile phone and/or SIM card, to which the mobile phone number is linked, provided by the Client to the Bank in order to receive SMS messages with OTP codes;*
 - *the loss (theft) of a token;*
 - *the attempts to unauthorized access to the Client's Account using the “KICB” system;*

The Client shall be obliged to immediately notify the Bank of this either through a written application or by telephone, provided that the Client specifies a code word or other supporting data (the list of identification data is established by the Bank), followed by written confirmation of this requirement within 5 (five) calendar days (application on paper with the signature and seal (if any) of the Client). If the Client is not able to provide the above written confirmation within 5 (five) calendar days, then this period may be changed by agreement with the Bank;

4.4.4. The Client shall be obliged not to allow on the devices used to enter “KICB” system, the loading of resident programs that allow uncontrolled access to storage devices and input/output devices;

4.4.5. The Client shall be obliged to use anti-virus software on the devices used to log into “KICB” system, keep the anti-virus software databases up to date, regularly install security updates issued by the developers of the operating systems and web browsers used;

4.4.6. The Client undertakes not to use the Bank's application on mobile devices (mobile phone and/ or other device allows the use of the Bank's application), which were subject to the process of obtaining full access to the operating system and all functions of the mobile device, which entailed the removal of restrictions by the manufacturer or telecom operator for manipulating system applications and provided ability to run applications that require administrator rights (root and/ or jailbreak).

4.5. The Bank shall not send messages and call the Client with a request to inform all or part of the Authorization Data. The Client, in turn, undertakes not to respond to incoming oral phone calls or written requests to report all or part of the Authorization Data. If the Client receives such requests, he is obliged to leave it unfulfilled/answer, and notify the Bank of this fact as soon as possible.

4.6. Only registered Clients can have Access to the “KICB” system and its use, including any Operations, as well as viewing information. The Client can't transfer his/her Authorization data to third parties; it's a direct violation of these Rules. The Client shall bear a full responsibility for the consequences of the transfer of his/her Authorization data to third parties. In case of revealing the fact of the Client's transfer of his/her Authorization Data to third parties, the Bank has the right, at its discretion, to temporarily suspend the Client's access to the “KICB” system or to completely terminate the provision of remote banking services to the Client in a unilateral extrajudicial procedure.

4.7. The Bank shall be entitled, without notifying the Client, to temporarily suspend or restrict the Client's access to “KICB” system, to refuse the Client to grant or renew access to “KICB” system if the Bank has sufficient grounds to believe that an attempt to unauthorized access to “KICB” system is possible on behalf of the Client.

4.8. The Bank is entitled to suspend the Client's access to “KICB” system in case if it was established that the Client has violated these Rules by blocking his/her account.

4.9. The client is informed and fully aware that the transmission of confidential information over the Internet entails the risk of unauthorized access to such information by third parties. After connection to “KICB” system, the Client shall agree with banking services via the Internet, realizing that the Internet is not a secure channel of communication and information transfer, as well as all the risks associated with a possible violation of confidentiality and other risks arising from the use of such a communication channel.

4.10. The Client shall understand that at use of “KICB” system there is a risk that third parties can have unauthorized access to the Client's accounts, as well as to information on Operations. Unauthorized access becomes possible due to the interception by third parties of the control of the Client's personal computer, mobile phone, theft of Authorization data.

4.11. The Client shall be obliged to fulfill the requirements of these Rules in full, as well as to take all necessary measures to secure and protect information and documents exchanged within the framework of “KICB” system.

4.12. The client shall be obliged to ensure the connection of his/her technical means (personal computer, mobile device and other means) to the Internet independently and at his/her own expense, as well as to ensure the protection of his/her own technical means from unauthorized access and malicious software.

4.13. If the Client violates the rules for the safe use of remote banking services specified in these Rules, as well as in cases of fraudulent transactions, hacker, virus attacks from the Internet, the Bank shall not be responsible for the Operations performed on the Client's Account.

5. Transactions

5.1. The Parties shall recognize Bishkek time (UTC+6) as a single time scale during work with the “KICB” system.

5.2. The transactions shall be carried out on the basis of the list provided by the Bank for the “KICB” system.

5.3. The Bank has the right to notify the Client about potentially important information for the Client by means of SMS messages, e-mail mailing, Push-notifications: about the Account status, about the movement of funds on the Account, with a reminder about loan debts, about new services of the Bank, etc.

5.4. The Bank shall provide the Client, who has Internet access with the following services/operations:

5.4.1. transfers within the Bank;

5.4.2. transfers to other banks in national currency;

5.4.3. transfers to other banks in foreign currencies;

5.4.4. currency conversion;

5.4.5. payments for the purpose of paying for services (utility bills, etc.);

5.4.6. other services/operations available to the Client.

5.5. The Bank shall be entitled to change the list of services provided through “KICB” system. When the Bank changes the list of services provided by the Bank through the “KICB” system, the Bank shall notify the Client by posting information on the Bank's website and/or an information message sent to the Client's email address in the manner prescribed by these Rules. The client has the right, at his discretion, to use or refuse these services.

5.6. Transfers of funds in a currency other than the currency of the Account (if the currency of funds in the Account is different and the currency of the funds transferred) shall be carried out at the exchange rate established by the Bank at the time of the Operation.

5.7. The Parties acknowledge that electronic payment documents (Client's Orders) executed in the “KICB” system are considered outgoing from the Client and are legally equated to payment documents received by the Bank from the Client in hard copy, drawn up in accordance with the regulatory legal acts of the Kyrgyz Republic and personally signed by the Client.

5.8. The Bank has the right to impose permanent or temporary restrictions for the performance of Operations through the “KICB” system. The Bank shall inform the Client about existence of restrictions by means of:

5.8.1. posting the documents and information on the Bank's website;

5.8.2. sending information messages in the Personal Account;

5.8.3. other ways at the discretion of the Bank, allowing the Client to receive information and establish that it's received from the Bank.

5.9. The Bank shall have the right to refuse to execute the Client's Order:

5.9.1. if there are not enough funds on the corresponding Client's Account to carry out this Operation, taking into account the commission (if any) for its execution;

5.9.2. if there is a suspicion in security violation during use of the “KICB” system, including if the Bank has reason to believe that the execution of the Order may result in financial losses for the Bank or the Client;

5.9.3. if the amount of Operation exceeds the limit (s) for Operations via the “KICB” system or does not comply with the limits established by the Bank's Tariffs;

5.9.4. if the acceptance of the Order is impossible without the provision by the Client of additional documents required in accordance with the legislation of the Kyrgyz Republic;

5.9.5. if the execution of the Order entails a violation of the current legislation of the Kyrgyz Republic, regulations of the National Bank of the Kyrgyz Republic, these Rules, as well as the terms of other agreements (contracts) concluded between the Client and the Bank;

5.9.6. if the Client's Account has been seized;

5.9.7. in other cases stipulated by the agreement concluded between the Bank and the Client and/or the legislation of the Kyrgyz Republic.

5.10. The Client agrees that use of his/her Authorization data is reliable and sufficient for establishment of his/her personality and confirmation of right to hold operations on his/her accounts.

5.11. Commission of the Bank paid by the Client in a currency other than the currency of debiting shall be carried out at the exchange rate established by the Bank at the time of the Operation.

6. Rights and obligations of the parties

6.1. The Bank shall be obliged to:

- 6.1.1. execute the Client's Orders, created during the Authorized session of work, on behalf of and at the expense of the Client;
- 6.1.2. advise the Client on the connection, use and performance of Transactions in “KICB” system;
- 6.1.3. provide technical support and maintenance of “KICB” system;
- 6.1.4. in case of technical problems in the process of “KICB” system use, to take all possible actions to eliminate them within a reasonable time, while the Client is not entitled to have claims to the Bank and during the period of elimination of technical problems must carry out Operations in the usual way using paper media, or use an alternative method of transferring the Client's Orders to the Bank;
- 6.1.5. to notify the Client about changes in the operation of “KICB” system in the manner prescribed by these Rules;
- 6.1.6. to keep bank secrecy about operations performed on the Client's accounts and provide information on them only in cases stipulated by the legislation of the Kyrgyz Republic;
- 6.1.7. to block access to the “KICB” system upon the written application of the Client (applicable only for legal entities). The Client's oral statement on blocking is accepted by the Bank upon proper identification of the Client - the Client's message of the code word or other identification data (applicable for individuals).
- 6.1.8. monitor the security of their own systems and take all possible measures to prevent hacking of systems and other external threats and attacks;
- 6.1.9. to bear other obligations stipulated by these Rules.

6.2. The Bank shall be entitled to:

- 6.2.1. unilaterally make changes and additions to these Rules (including in connection with the emergence of new services/services/opportunities), or establish new Bank Tariffs with notification of the Client about this by posting electronic versions of new versions of the Bank www.kicb.net 10 (ten) calendar days prior to the date of entry into force of these amendments or additions, with the exception of amendments and additions due to the requirements of the legislation of the Kyrgyz Republic, an earlier date of entry into force provided for by the regulatory acts of the Kyrgyz Republic;
- 6.2.2. at its own discretion, temporarily suspend or restrict the Client's access to the “KICB” system or refuse to grant or renew access to “KICB” system, or refuse to carry out specific Operations, or unilaterally and out of court completely terminate or temporarily suspend the provision to the client of remote banking services:
 - 6.2.2.1. in case if it was found that the Client's actions clearly indicate the presence of malicious intent, with the aim of causing damage to the Bank;
 - 6.2.2.2. in case of detection of facts of violation by the Client of the security rules and conditions for using the “KICB” system, set forth in these Rules, as well as the current legislation of the Kyrgyz Republic;
 - 6.2.2.3. if the Customer has unpaid debt to the Bank, including overdue debt on loans;
 - 6.2.2.4. in case of insufficient funds on any Account for payment of the cost of services using the “KICB” system;
 - 6.2.2.5. in case if the Client has violated the terms of these Rules;
 - 6.2.2.6. in case of technical malfunctions while working with the “KICB” system;
 - 6.2.2.7. in case of change of software and carrying out preventive maintenance;
 - 6.2.2.8. in case of a disputable situation related to service of the Customer at the Bank, until the dispute is resolved;
 - 6.2.2.9. in other cases provided for by these Rules, the legislation of the Kyrgyz Republic;

6.2.3. unilaterally establish and change limits for the performance of Operations through “KICB” system, establish technical and other restrictions, as well as implement other mechanisms that reduce the risks of the Client and the Bank arising from the use of the “KICB” system, including additional organizational and technical measures to increase the level of security in the provision of remote banking services;

6.2.4. without Client’s consent, order and payment orders (in a non-authoritative manner), as a matter of priority, write off funds from any Client’s Account, to which the Client expresses his/her unconditional consent:

6.2.4.1. for payment of services and commissions of the Bank and other banks related to service of the Client and Transactions, carried out on the Client’s Account (s), on the day of the Operation/provision of the service or at any time after the completion of the Operation/provision of the service, in accordance with the current Tariffs of the Bank regardless of the presence of facts of using the “KICB” system and/or operations on the Client’s Account;

6.2.4.2. to compensate for the Bank’s expenses incurred in the course of business relations with the Client or in connection with remote banking services for the Client;

6.2.5. immediately cancel the Client’s access to the “KICB” system, in case of closing the Client’s Account (s) with the Bank;

6.2.6. if necessary, request the Client to issue the Client’s Order on hard copy with the signature of the manager/authorized persons and the seal of the Client (if any) for the implementation of the service/operation no later than the next business day by sending the Client a written message or an information message sent to Personal account. In this case, the Bank will not execute the Client’s Order until the receipt of the document in hard copy;

6.2.7. disconnect the Client (legal entity) from the “KICB” system if the legal entity has a debt to the Bank for more than 3 (three) months to maintain a current account using the “KICB” system. To re-connect the Client to the “KICB” system, the Client will have to pay a fee for connection based on the Bank’s Tariffs;

6.2.8. in case of expiration of the passport switch the Client’s access in the “KICB” system to the “View mode” until the Client submits a valid passport to the Bank;

6.2.9. in case of expiration of the Client’s power of attorney, close access to Client in “KICB” system;

6.2.10. exercise other rights provided for by these Rules.

6.3. The client shall be obliged to:

6.3.1. bear responsibility for observing confidentiality (transfer/disclose) the authorization data to third parties, to ensure the storage of Authorization Data in a way that excludes the possibility of unauthorized access to it by unauthorized persons. If the Client has the slightest suspicion or revealed facts indicating the above, the Client is obliged to immediately notify the Bank either by written application or by telephone, provided that the Client indicates a code word or other supporting data (the list of identification data shall be established by the Bank), followed by within 5 (five) calendar days by written confirmation of this requirement (application on paper, signed and sealed (if any) by the Client). In case if the Client has no possibility to provide the above written confirmation within 5 (five) calendar days, then this period may be changed based on agreement with the Bank;

6.3.2. ensure the balance of funds on the Account required to pay for the Bank’s services on time and in accordance with the Tariffs for servicing the “KICB” system;

6.3.3. inform the Bank in writing about all changes in the information specified in the Application, no later than 3 (three) business days from the date of their change with the attachment of the necessary supporting documents;

6.3.4. perform Operations on the Account in accordance with the current legislation of the Kyrgyz Republic, comply with these Rules, including a set of measures to comply with security rules when using “KICB” system;

6.3.5. pay for the services and commissions of the Bank for remote banking services and execution of Account Operations in accordance with the Bank’s Tariffs, as well as pay for the services of other banks

involved in the process of the Client's Account Operations, and any other costs associated with servicing the Client and performing Operations;

6.3.6. in case of replacement of the mobile phone number provided by the Client to the Bank in order to receive SMS messages with OTP codes, to notify the Bank in writing about this;

6.3.7. check the status of the Operations after sending the Client's Orders to the Bank;

6.3.8. inform the Bank in writing about the change of managers and/or authorized persons to manage the Account within 3 (three) business days from the date of such replacement;

6.3.9. at the request of the Bank, no later than 5 (five) calendar days (from the date of receipt of such a request), submit to the Bank all payment documents, transacted using “KICB” system on hard copy, certified by the Client and sealed by the Client (if any);

6.3.10. bear other obligations stipulated by these Rules.

6.4. The Client shall be entitled to:

6.4.1. use the full range of services of the “KICB” system on conditions stipulated by these Rules;

6.4.2. receive advice from the Bank on the connection and use of the “KICB” system;

6.4.3. install and change the Authorization data for using the “KICB” system on a regular basis;

6.4.4. exercise other rights provided by these Rules.

7. Responsibility of the parties and settlement of disputes

7.1. The Bank shall take all possible measures to resolve the dispute that has arisen within the framework of using the “KICB” system and notify the Client about the results.

7.2. Disputes and disagreements that arise from the execution of these Rules shall be resolved through negotiations between the Client and the Bank. If it is impossible to resolve the dispute out of court, it shall be resolved in court in accordance with the current legislation of the Kyrgyz Republic.

7.3. If necessary, in order to resolve a dispute, the Bank may involve various specialists and experts (both employees and not-employees of the Bank) who have the necessary experience and knowledge in the relevant field.

7.4. The parties shall be responsible for non-fulfillment or improper fulfillment of their obligations stipulated by these Rules in accordance with the legislation of the Kyrgyz Republic and these Rules.

7.5. The client shall be responsible for the device used to connect to “KICB” system, for using only licensed software with the latest updates installed, as well as licensed anti-virus software with up-to-date anti-virus databases on the used device.

7.6. The Client shall be responsible for losses incurred by the Bank as a result of the execution of Orders submitted to the Bank on behalf of the Client by an unauthorized person.

7.7. The Client shall be responsible for untimely and/or incomplete written notification of the Bank about the circumstances that are important for provision of services within the framework of remote banking, including changes in the information previously reported to the Bank. The Client shall bear a full liability for possible negative consequences in case of untimely or incomplete notification of the Bank about such circumstances.

7.8. By accepting these Rules, the Client expresses his/her unconditional consent that the Bank is not responsible for:

7.8.1. errors, delays or inability of the Client to have access to “KICB” system associated with a malfunction of the Client's equipment (Wi-Fi router/modem, etc.) or communication channels, technical means, other resources and services by means of which services are performed in “KICB” system, provided by a third party (providers of Internet access, communications, etc.);

7.8.2. damage to the Client's equipment, for the safety of the Client's software and personal computer from various viruses and other damages, for the safety of the mobile phone and other devices of the Client from various viruses and other damages;

7.8.3. consequences of the untimely notification of the Bank by the Client about the loss (theft) of a login and/or password, a mobile phone/SIM card to which the mobile phone number is linked, provided by the Client to the Bank in order to receive SMS messages with OTP codes, a token, about incorrectly produced Operations and attempts to unauthorized access to the Client's Account using the “KICB” system. The Client shall be responsible for any losses and liability due to such actions.

7.8.4. consequences of not notifying the Bank by the Client of a change in the phone number to receive an SMS message with OTP codes, details (including the postal address) specified by the Client in order to receive information;

7.8.5. non-fulfillment of the Client's payment orders in the “KICB” system, if the order was submitted not in full (incorrect) format and/or included information that contradicts the current legislation of the Kyrgyz Republic;

7.8.6. damage caused by the Client's disclosure of the Authorization Data, the Client's failure to ensure their confidentiality or the Client's failure to take measures to keep them secret from third parties, transfer them to third parties, regardless of the reasons;

7.8.7. Client's losses caused by the Bank's execution of Orders for Transactions from unauthorized persons made as a result of access to “KICB” system by third parties, in cases where such access occurred in a situation that is not subject to or isn't controlled by the Bank (compromise of the Client's logins and passwords);

7.8.8. Client's losses caused by the Bank's execution of Orders for Transactions from unauthorized persons committed as a result of the use of the Client's Authorization Data by third parties, including those obtained by illegal methods, violation of the confidentiality of the Client's Authorization Data, including caused by information leakage directly from the Client's device used to access the “KICB” system, malicious software installed on the device used by the Client to access the “KICB” system, fraudulent, hacker, virus attacks from the Internet;

7.8.9. Client's losses caused by the execution by the Bank of Orders for the performance of Operations from unauthorized persons received by the Bank as a result of access and use of the “KICB” system by third parties, if this happened not through the fault of the Bank;

7.8.10. impossibility of providing the “KICB” system, if such occurred due to force majeure circumstances beyond the Bank's control, including but not limited to failures in provision of communication on the side of Internet providers;

7.8.11. failure to use the mobile phone by the Client due to the breakdown and/or loss/theft of the SIM card, for the malicious action of the software installed on the Client's mobile phone, which resulted in the compromise of OTP codes, for damage caused by unauthorized use of OTP codes by the Client's third parties;

7.8.12. in case if information transmitted when using the “KICB” system, including about Accounts, becomes known to third parties as a result of listening or interception of communication channels during their use, as a result of third parties' access to information during transmission via communication channels used by the Client, as well as in case of unfair fulfillment by the Client of the conditions for storage and use of funds for Authentication;

7.8.13. the quality of delivery of SMS messages to the Client's mobile phone, for the delivery and transmission speed of SMS messages and does not guarantee the preservation of the confidentiality and integrity of information transmitted in the form of SMS messages. The Bank shall not be responsible for failures, accidents and overloads in the operation of mobile/mobile radiotelephone networks, failures and delays in the operation of mobile radiotelephone operators, problems with the Client's use of mobile/mobile radiotelephone communications in roaming, that is, outside the communication network of the mobile operator/mobile radiotelephone communication;

7.8.14. in case of arbitrary or deliberate interference of third parties in the private affairs of the Client (including those related to the civil law relations of the Client with the Bank), carried out through unfair use by a third party of the means of communication and contact information of the Client provided by the Client to the Bank. The Bank shall not be responsible for the transfer by the Client to third parties of a mobile phone (SIM-card), illegal production by third parties of a duplicate of the Client's mobile phone and/or SIM-card and use of this SIM-card without Client's knowledge and consent;

7.8.15. in case if the Client fails to receive information sent by the Bank to him/her in cases established by these Rules, if the contact information transmitted to the Bank by the Client has become irrelevant, information about which was not brought to the Bank by the Client in a timely manner and in the manner prescribed by the Bank. The Bank shall not be responsible for non-fulfillment, untimely or incorrect execution of Orders and/or the Client Authentication procedure, if it was caused by the provision of false information by the Client, loss of relevance of information previously provided by the Client and used during registration and fulfillment by the Bank of its obligations within the OTP-mailing list. Codes or incorrect data entered by the Client. The Client shall be responsible for the correctness and relevance of all information provided to the Bank;

7.8.16. non-fulfillment of the Client's Orders using “KICB” system, if the Client's Account was seized or the Operations on it were suspended in accordance with the current legislation of the Kyrgyz Republic, as well as in other cases stipulated by the legislation of the Kyrgyz Republic;

7.8.17. losses incurred by the Client as a result of the execution by the Bank of the Client's Order drawn up by the Client with errors and/or typographical errors in the information contained in the fields of the document, as well as in case if the Client's payment is returned by the receiver;

7.8.18. execution of the Orders erroneously sent by the Client;

7.8.19. for non-fulfillment, untimely or incorrect execution of the Order, if this was caused by the provision by the Client of inaccurate information, the loss of the relevance of information previously provided by the Client and used for the Client's Authorization, or the Client entered incorrect data;

7.8.20. non-execution of the Client's Order, if its execution would lead to a violation of the requirements of the current legislation of the Kyrgyz Republic, these Rules, as well as the terms of other agreements (contracts) concluded between the Client and the Bank.

8. Force-Majeure

8.1. The parties shall be exempt from liability for full or partial failure to fulfill their obligations if such failure was the result of force majeure circumstances (force majeure), that is, events that could not have been foreseen or prevented. Force majeure circumstances include, but are not limited to: natural disasters, fires, floods, earthquakes, other natural or man-made disasters, epidemics, hostilities, coups d'état, the imposition of a state of emergency, revolutions, riots, terrorist acts, civil unrest, actions Governments, state bodies, the National Bank of the Kyrgyz Republic, normative acts that entered into force after the date of conclusion of this agreement for remote banking services, the adoption by the National Bank of the Kyrgyz Republic and/or state authorities of the Kyrgyz Republic of a decision that entailed the impossibility of the respective Party to fulfill its obligations, as well as other circumstances beyond the reasonable control of the Parties.

8.2. The occurrence of force majeure circumstances shall entail an increase in the term for the fulfillment of the corresponding obligations for a period commensurate with the time during which such circumstances were in effect.

8.3. Documents issued by authorized state bodies will be an appropriate proof of force majeure circumstances. Proofs of the force majeure circumstances are provided by the Party referring to the force majeure circumstances, at the request of the other Party.

9. Final Provisions

9.1. Seizure of the Account or suspension of operations on the Client's Account at the request of the authorized law enforcement/state bodies in cases stipulated by the legislation of the Kyrgyz Republic, blocks the operation of the “KICB” system until the restrictions are stopped.

9.2. The client can disconnected the “KICB” system at his/her own request within 5 (five) business days after submitting a corresponding written application to the Bank.

9.3. If the Client disconnects “KICB” system at his/her own request, or at the initiative of the Bank (as a result of non-compliance/violation of these Rules; in cases stipulated by law), the Bank shall block the possibility of using “KICB” system by the Client.

9.4. With regard to all other respects that are not provided for by these Rules, the Parties shall be guided by the requirements of the legislation of the Kyrgyz Republic.