Approved by the Minutes of the Board
No. 29 (3) as of June 15, 2021
Entered into force on June 15, 2021

PUBLIC OFFER

Regulations on the Provision and Use of Remote Banking Services

1. General provisions

1.1 These Regulations on the Provision and Use of Remote Banking Services (hereinafter – the Regulations) are a public offer which is an offer to conclude Remote Banking Services Agreement using the systems "Internet Banking" and/or "Mobile Banking" on the terms specified in these Regulations.

1.2 For the purpose of entering into the Remote Banking Service Agreement on the terms specified in these Regulations and using remote banking services (hereinafter referred to as RBS), the Client unconditionally accepts and joins these Regulations by submitting an Application for remote banking services (hereinafter referred to as the Application) in the form approved by OJSC "Keremet Bank" (hereinafter referred to as the Bank), both in writing and in the form of an electronic document signed with a simple electronic signature.

1.3 These Regulations define the procedure for providing by the Bank with the services of "Internet Banking" and "Mobile Banking" making transactions by Clients in the systems of "Internet Banking" and "Mobile Banking" as well as regulate the relations arising between the Client and the Bank in the provision and use of remote banking services. The Regulations are binding on both the Client and the Bank.

1.4 The Client hereby confirms that:

1.4.1. prior to submitting an Application to the Bank he/she has fully read and agrees with these Regulations and the Bank's Tariffs for services rendered, undertakes to comply with them and monitor changes in the Bank's Tariffs and these Regulations on the Bank's website www.keremetbank.kg;

1.4.2. he/she is aware of and agrees that Bank is entitled to unilaterally modify or amplify these Regulations, to change or impose new Tariffs of the Bank notifying the Client about it by posting electronic versions of new editions of these documents on the Bank's website www.keremetbank.kg 10 (ten) working days prior to the effective date of these changes or additions have taken effect, except for the amendments caused by requirements of legislation of the Kyrgyz Republic, earlier period of entry of which is provided by the normative acts of the Kyrgyz Republic;

1.4.3. he/she is familiar with and undertakes to comply with the safety requirements for the provision of remote services provided by these Regulations and Annex No. 1 to these Regulations;

1.5 Client who has enacted these Regulations assumes all rights and obligations provided by these Regulations.

1.6 When the Client logs in to the Internet Banking and/or Mobile Banking and before starting the service, the Client should read the current version of these Regulations posted on the Bank's website www.keremetbank.kg. Authentication of the Client in the System, receipt by the Client of the Internet Banking and/or Mobile Bank services means acceptance by the Client of these Regulations in full and consent of the Client to all their provisions.

1.7 By connecting to the remote banking service the Client agrees to banking services via the Internet, realizing that the Internet is not a secure communication channel and the Client enacting these Regulations assumes all risks:

1.7.1. arising from the use of such a channel of communication including possible access by third party to Authorization data of the Client and committing to a third party who have knowledge of authorization data of the Client, expenses and other transactions on Account(s) of the Client and other actions for managing Client's Account (s);

1.7.2. related to the connection of technical means to the Internet and independently protects his/her own technical means from unauthorized access and malicious software;

1.7.3. The Client assumes all possible wastes, losses, damages, etc. arising from the use of remote banking services via the Internet including as a result of fraudulent, hacker, virus attacks from the Internet and hereby warrants that he/she will not lodge claims to the Bank or file any claims against it in such cases as the Bank has previously and fully informed the Client about possible risks. The Client hereby acknowledges and confirms that he/she is a proponent of providing with technical ability to manage the Account (s), dispose of the funds in the Account (s) and make payments and transactions using remote banking services, as well as the fact that he/she releases the Bank from any liability, and the Bank respectively shall not be liable for any consequences that may arise for the Client in the event of interception by third parties of personal control of Client's computer, mobile phone, theft of authorization data or non-compliance with security procedures by the Client;

1.8 Types and amount of commissions to be paid by the Client when using remote banking services are 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 and conditions specified in these Regulations.

1.9 The Client has the right to refuse use of the RBS by filing applications at the point of sale of the Bank in the absence of disputed transactions, debt payment service of the Bank and third party banks involved in the implementation of Client's operations, other outstanding obligations to the Bank and any other claims of the Bank related to remote banking services of the Client and his/her Accounts.

1.10 Requirements for blocking access to the remote banking system received by the Bank in the manner prescribed by these Regulations are recognized by the parties as coming from Client and claims for the consequences of blocking by the Bank are not accepted, because the Client by enacting these Regulations and by submitting an Application to the Bank expresses his/her unconditional consent.

2. Terms and definitions

2.1 Authorized work session is the period of Client's work in the System, the beginning of which is Client's authentication procedures. End of the authorized session of the Client in the System is the moment of exit from it.

2.2 Authorization data are login and password, OTP, PIN and biometric data of the Client used by the Bank to authenticate the Client when entering the system.

2.3 Client Authentication is the authentication of the Client by verifying the authenticity of the presented identifier (PIN, login, etc.) based on the authorization data.

2.4 Bank is OJSC "Keremet Bank".

2.5 Biometric data is a fingerprint read and processed by a mobile phone used to authenticate the Client. It is an optional replacement for the PIN available if the Client's mobile phone supports such functionality.

2.6 Remote banking service (RBS) is a complex of services of remote access of the Client to the products and services of the Bank, which also allows you to manage your own Accounts and funds on them. It includes following services:

- Internet Banking is a remote service channel providing the Client with the opportunity to receive and use the Bank's products and services via the Internet through a web browser installed on a personal computer;
- Mobile Banking is a remote service channel providing the Client with the opportunity to receive and use the Bank's products and services via the Internet through a mobile application;

2.7 Application is application for remote banking services.

2.8 User name (thereinbefore and hereinafter also login) is a unique sequence of alphabetic (Latin) characters used to authenticate the Client in the system. Initially user name (login) is generated by the Bank when connecting to the remote banking service, then it can be changed by the Client.

2.9 The Client is a person specified in the Application who has been granted the right to use remote banking services in accordance with these Regulations.

2.10 Transaction is any banking transaction carried out by the Bank at Client's Order.

2.11 One-time digital password (One Time Password, hereinafter OTP) is a unique sequence of digital characters sent to Client's mobile phone via SMS or generated by the mobile application Google Authenticator in cases provided for by these Regulations to authenticate the Client.

2.12 Password is a unique sequence of characters used to authenticate the Client in the system. Password is used repeatedly and has a limited validity period established by the Bank at the end of which the Client is obliged to change Password.

2.13 PIN is a unique sequence of digital symbols used to authenticate the Client in the Mobile Banking service. PIN replaces Login and Password after first successful authentication of the Client.

2.14 A simple electronic signature is an electronic signature whose signature key matches the electronic signature itself (codes, passwords, and other identifiers). Simple electronic signature is considered equivalent to the Client's handwritten signature.

2.15 Client's Order is an electronic payment document containing the Client's instruction to the Bank to perform banking operations provided for by these Regulations and functionality of Internet Banking and/or Mobile Banking.

2.16 System or DBO System is a software and hardware complex that provides DBO services to the Clients.

2.17 Parties are the Bank and the Client.

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

2.19 Tariffs are list of services established by the Bank and amount of remuneration (commissions) charged for the services. The applicable tariffs are communicated to the Client in accordance with paragraph 1.4.2. of these Regulations.

2.20 Authorized person - Client is a natural person, a representative of the Client is a legal entity empowered to manage Client's Accounts, dispose of funds on these Accounts on behalf of and at the expense of the Client, to perform Operations on Client's Account, to receive information about balances on Client's Accounts, as well as to receive statements of cash flows on Client's Accounts.

2.21 Google Authenticator is a mobile application installed on Client's mobile phone and used to generate OTP.

2.22 Point of sale of the Bank is a structural division of the Bank engaged in direct work with Clients.

2.23 Push notification is a message sent by the Bank using the Internet to a mobile device with the Mobile Banking application installed on it.

2.24 Electronic document is a documented information presented in electronic form and having the appropriate details for verification of authenticity, suitable for transmission over information and telecommunications networks and processing in information systems.

2.25 **Electronic signature** is an information in electronic form that is attached to other information in electronic form and (or) logically related to it and which is used to determine the person on whose behalf the information is signed.

3. Procedure for granting access and use of the system

3.1 Right to use the Internet Banking and/or Mobile Banking is provided by the Bank to the Client personally and is not transferable to third parties. Client's authorized persons are not third parties.

3.2 Initially password is generated by the Bank when connecting to the RBS. Client can change password an unlimited number of times at his/her discretion after the first successful authentication subject to the requirements for complexity of password (described below).

3.3 OTP can be sent to Client's mobile phone via SMS or it can be generated via Google Authenticator mobile application.

3.4 Method of obtaining OTP is chosen by the Client at the time of submitting the Application to the Bank and can be subsequently changed at the request of the Client.

3.5 Client's access to the Internet Banking service is carried out via the Internet via a web browser. The system supports the following web browsers: Internet Explorer, Firefox, Google Chrome, Opera, Safari. It is mandatory to use the most current versions of these web browsers at the time of authorization.

3.6 Client's access to the Mobile Banking service is carried out via the Internet through the application installed on mobile phone. This application is only supported by following mobile operating systems: iOS and Android.

3.7 All Transactions made through the RBS within an authorized session are unconditionally recognized by the Parties as transactions made personally by the Client or his/her authorized person and the Client bears full financial responsibility for such transactions.

3.8 All actions in the RBS both to obtain information and to perform transactions within an authorized session are unconditionally recognized by the Parties as committed personally by the Client or his/her authorized person and the Client bears full financial responsibility for such transactions.

3.9 Information recorded in the Minutes of the Bank's information systems on transactions made within an authorized session of work shall be recognized by the Bank and the Client as a documentary source confirming facts of Client's transactions in the system and gives cause for Bank's settlements on Client's orders, as well as calculation, debiting from Client's Account or reclaiming from Client the commissions due to the Bank in accordance with the Tariffs and these Regulations.

3.10 The Client is obliged to treat the transactions through the RBS with due care, as well as to take reasonable measures to reduce the likelihood of unintentional or accidental transactions in the system. All transactions made during an authorized session, including payment for goods/services, transfers and payments are considered to be executed at Client's order and confirmed by him/her.

4. Basic security and privacy requirements

4.1 This section defines the rules that are mandatory for the Client to comply with in order to ensure the necessary level of security when using the RBS, and also includes a list

of measures to ensure the confidentiality of client data and operations performed by the Client.

4.2 The Bank exercises and the Client acknowledges the Bank's right to store in the electronic logs of the Bank's systems all events and actions performed within the authorized session.

4.3 The Bank complies with safety requirements when the Client using RBS by the following measures:

- mandatory assignment of a unique Login to each Client serving the purposes of client authentication in the system;
- mandatory Password generation by methods that exclude the possibility of access to Password information for any third parties;
- setting password complexity requirements, namely:
  - Password length is not less than 9 (nine) and not more than 25 (twenty-five) characters;
  - Minimum presence of 1 (one) character in each case (low, high);
  - Minimum 1 (one) number in Password;
- limiting the number of attempts to enter the Password for the Internet Banking in case of its wrongness, namely:
  - Initially, for entering Password is given 3 (three) attempts, in case of entering wrong Password 3 (three) times in a row the Internet Banking is blocked for 15 (fifteen) minutes;
  - After the period of the first blocking are given 3 (three) more attempts, in case of entering an incorrect Password 3 (three) times in a row the Internet Banking is blocked for 15 (fifteen) minutes;
  - Upon expiration of the second blocking period are given 3 (three) more attempts, in case of entering an incorrect Password 3 (three) times in a row the Internet Banking is prematurely blocked and can be unlocked only upon written application of the Client.
- limiting the number of attempts to enter PIN for the Mobile Banking in case of its wrongness, namely:
  - Initially, for entering PIN is given 3 (three) attempts, in case of entering wrong PIN 3 (three) times in a row the Mobile Banking is blocked for 15 (fifteen) minutes;
  - After the period of the first blocking are given 3 (three) more attempts, in case of entering an incorrect PIN 3 (three) times in a row the Mobile Banking is blocked for 15 (fifteen) minutes;
  - After the period of the second blocking are given 3 (three) more attempts, in case of entering the wrong PIN 3 (three) times in a row, the Client must re-pass the authentication procedure and receive a new PIN.
- mandatory OTP input;
- use of Client's biometric data as authorization data for the Mobile Banking Service if such functionality is supported by Client's device;
- setting an OTP code validity time limit of 30 seconds;
- other methods previously or in the future established by a responsible person as ways to increase the level of information security of the service.

4.4 On behalf of the Client the following measures are mandatory to ensure information security when the Client uses the RBS:

- The Client must necessarily keep Login, Password, OTP, PIN confidential. It is strictly forbidden to transfer authorization data to third parties in oral or written form;
- The Client must change the password on a regular basis within an authorized session;

- If the Client has the slightest suspicion or revealed facts indicating: access of third parties to the Client's authorization data, access of third parties to the RBS on behalf of the Client, loss (theft) of the mobile phone and/or SIM card, to which the mobile phone number is linked, communicated by the Client to the Bank in order to receive SMS messages with OTP codes, attempts of unauthorized access to the Client's Account using the Internet Banking and/or Mobile Banking, the Client must immediately contact the Bank with a request to block access to the RBS by phone **+996 (312) 55 44 44** or by email to call-center@keremetbank.kg with the notification of the Client's identity data, followed by a written confirmation of this requirement within 5 (five) calendar days (application in hard copy, signed and sealed (if available) by the Client). If the Client does not have the opportunity to provide the above-mentioned written confirmation within 5 (five) calendar days, this period may be changed by agreement with the Bank;
- Access to RBS can be unlocked only upon written application of the Client (application on paper signed and sealed (if available) by the Client);
- The Client is obliged to get acquainted in a timely manner with the information communicated by the Bank to clients by methods specified in paragraph 6.2.1 of these Regulations, also in terms of information relating to possible risks when using the service, and to take all necessary actions in connection with the above information if required;
- The Client undertakes not to allow on devices used for system entry loading of resident programs allowing uncontrolled access to devices of accumulation of information and devices of input/output;
- The Client undertakes to use the anti-virus software in monitor mode on devices used for system entry to keep the anti-virus software databases up to date, to regularly install critical security updates issued by developers of the operating system and web browser used.

4.5 The Bank does not send and the Client undertakes not to respond to incoming oral or written requests to report all or part of the authorization data. If the Client receives such a request, he/she is obliged to leave it without execution/response and notify the Bank of this fact as soon as possible.

4.6 Access to the system and its use including the performance of any operations, as well as viewing information is allowed only to registered clients. Transfer of Client's authorization data to third parties is prohibited and is a direct violation of these Regulations. The Client is fully responsible for consequences of transferring his/her authorization data to third parties. In case of revealing of the fact of transfer by the Client of his/her login details to third parties the Bank may at its discretion suspend the Client's access to RBS or in a unilateral extrajudicial order to cease provision of the remote banking services.

4.7 The Bank shall have the right to temporarily suspend or restrict Client's access to the RBS without notifying the Client, refuse to grant or resume access to the RBS if the Bank has sufficient grounds to believe that an attempt of unauthorized access to the system on behalf of Client is possible.

4.8 The Bank shall have the right to suspend Client's access to the RBS by blocking his/her account in the event of a violation of these Regulations.

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. By connecting to the RBS, the Client agrees to banking servicing via the Internet with the awareness that the Internet is not a secure channel of communication and transmission of information, realizing all the risks associated with a possible breach of confidentiality and other risks arising from the use of such a communication channel.

4.10 The Client understands that there is a risk of unauthorized access to information on transactions by third parties when using the RBS. Unauthorized access becomes possible in connection with the interception by third parties of control of Client's personal computer, mobile phone, theft of authorization data.

4.11 The Client undertakes to fully comply with the requirements of these Regulations, as well as to take all necessary measures for the security and protection of information and documents exchanged within the framework of the RBS.

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

4.13 In case of violation by the Client of the rules on safe use of remote banking services specified in these Regulations, as well as in cases of fraudulent transactions, hacker, virus attacks from the Internet, the Bank shall not be liable for transactions made on the Client's Account.

5. Transactions

5.1 The Parties recognize Bishkek time as a single time scale when working with the system put down in electronic documents.

5.2 Transactions are carried out in the system based on list provided by the Bank for Internet Banking and Mobile Banking Services.

5.3 When using the service, the Bank also provides a package of services for obtaining information on accounts including the formation of account statements, information on the status of loans at the Bank, information on the list of account transactions, the list of transactions on Bank cards (hereinafter - the cards), account balances, available card balances within the authorized session.

5.4 The Parties acknowledge that the account statement provided by the Bank using the resources of the system is an official document confirming the banking transactions carried out by the Client on the account(s) including using the system. The Parties also agree that in the event of any disputes over the transactions conducted using the system the above account statement will be conclusive evidence including in court confirming the fact of Client's transactions on his/her account (s) and the fact of the Bank's transactions in accordance with Client's orders. Account statement shall be provided to the Client at his/her request not later than 5 (five) working days from the date of receipt of request by the Bank.

5.5 The Bank has the right to notify the Client about potentially important information for the Client by SMS messages, e-mail newsletters, push notifications: about the status of the account, about the movement of funds on the account, with a reminder of loan arrears, about new services of the Bank, etc.

5.6 The Bank with RBS shall provide the Client with remote access to accounts and the possibility of remote compilation and transmission to the Bank of Client's orders for transactions remote possibility of which is provided by these Regulations including:

- transfers between the Client's Accounts with the Bank;
- transfers from the Client's Account to accounts of third parties opened in the Bank;
- transfers from the Client's Account to the Client's accounts or third party's accounts opened in other banks;
- transfers from the Client's Account to third parties in order to pay for services (utilities, etc.);
- SWIFT transfers used for currency transfers (both international and within the Kyrgyz Republic);

5.7 The Bank has the right to change the list of transactions carried out through the Internet Banking and Mobile Banking. In this case the relevant changes are communicated to the Client in accordance with paragraph 6.2.1 of these Regulations.

5.8 Transfers of funds in a currency other than account currency (if currency of funds on the account and currency of transferred funds differ) are carried out at the exchange rate established by the Bank at the time of transaction.

5.9 The Parties acknowledge that electronic payment documents (Client's orders) issued in the system are considered to come from the Client and are legally equivalent to payment documents received by the Bank from the Client on paper issued in accordance with regulatory legal acts of the Kyrgyz Republic and personally signed by the Client.

5.10 The Bank has the right to impose permanent or temporary restrictions on transactions through Internet Banking and/or Mobile Banking. The Bank shall inform the Client of the restrictions by:

- placement of documents and information on the Bank's website www.keremetbank.kg;
- placement of documents and information on stands at the points of sale of the Bank;
- distribution of information messages by E-Mail;
- sending information messages via SMS;
- transfer Push notifications to the Client's mobile device;
- in other ways at the discretion of the Bank allowing the Client to obtain information and establish that it comes from the Bank.

5.11 The Bank has the right to refuse to execute the Client's order:

- if there are not enough funds on the relevant Client Account to perform this transaction taking into account the commission for its execution (if any);
- if there is a suspicion of a security breach when using the service including if the Bank has reason to believe that the execution of the order may entail financial losses for the Bank or the Client;
- if the amount of transaction exceeds limit(s) for transactions through the RBS or does not comply with the restrictions set by the Bank's tariffs;
- if acceptance of the order is impossible without providing by the Client with additional documents required in accordance with the legislation of the Kyrgyz Republic;
- if the execution of the order entails a violation of the current legislation of the Kyrgyz Republic, including Law on countering the financing of terrorist activities and anti-money legalization (laundering), regulations of the National Bank of the Kyrgyz Republic, these Regulations, as well as the terms of other agreements (contracts) concluded between the Client and the Bank;
- in other cases stipulated by the agreement concluded between the Bank and the Client and/or the legislation of the Kyrgyz Republic.

5.12 The Client agrees that the use of his/her authorization data is appropriate and sufficient to establish his/her identity and confirm the right to conduct transactions on accounts.

6. Rights and obligations of the Parties

6.1. The Bank is obliged to:

6.1.1. execute orders of the Client created during an authorized work session on behalf of and at the expense of the Client.

6.1.2. advise the Client on the connection and use of RBS and transactions in the system.

6.1.3. in case of technical problems in the process of using the RBS, take all possible actions to eliminate them within a reasonable time. In this case the

Client has no right to raise claims to the Bank and must carry out operations in the usual way using paper during the period of elimination of technical problems or use an alternative method of transferring the Client's orders to the Bank.

6.1.4. bear other duties provided by these Regulations.

6.2. The Bank is entitled to:

6.2.1. unilaterally make changes and additions to these Regulations (including in connection with the emergence of new services/feature/RBS opportunities) or to establish new Tariffs of the Bank notifying the Client about it by posting electronic versions of new editions of these documents on the Bank's website: ***www.keremetbank.kg***10 (ten) working days prior to the effective date of these changes or additions have taken effect, except for the amendments caused by requirements of legislation of the Kyrgyz Republic earlier period of entry of which is provided by the normative acts of the Kyrgyz Republic.

6.2.2. at its sole discretion temporarily suspend or restrict the Client's access to the RBS, refuse to provide or resume access to the RBS, refuse to conduct specific transactions or unilaterally out of court completely terminate the provision of remote banking services to the Client:

6.2.2.1. when identifying actions of the Client clearly indicating the presence of malicious intent in order to damage the information systems of the Bank;

6.2.2.2. in case of detection of the facts of violation by the Client of safety rules and conditions of use of RBS stated in these Regulations, also of current legislation of the Kyrgyz Republic;

6.2.2.3. in case of unpaid debts of the Client to the Bank including overdue loans;

6.2.2.4. if the Client violates the terms of these Regulations;

6.2.2.5. if the Client refuses to provide the documents required by the Bank, including the information and/or documents necessary for the proper verification of the Client and the execution of transactions;

6.2.2.6. in other cases stipulated by these Regulations and the legislation of the Kyrgyz Republic.

6.2.3. to unilaterally set and change limits on transactions through the RBS system, establish technical and other restrictions, as well as implement other mechanisms in the system that reduce the risks of Client and the Bank arising from the use of Internet Banking and Mobile Banking, including taking additional organizational and technical measures to improve the level of security in the provision of RBS;

6.2.4. to pause work of RBS system for carrying out procedure of change of the software and carrying out preventive works;

6.2.5. without the consent, without the order and without payment orders of the Client (in the non-acceptance order) to write off funds from the Client's Accounts as a matter of priority:

6.2.5.1. in payment of services and commissions of the Bank and other banks related to the Client service and Transactions on the Client's Account (s) on the day of transaction/provision of the service or at any time after transaction/provision of the service in accordance with the applicable tariffs of the Bank;

6.2.5.2. for compensation of expenses incurred by the Bank in business relations with the Client or in connection with remote banking services provided to the Client;

6.2.6. to restrict Client's access to the RBS system immediately in case of closing Client's Account (s) in the Bank.

6.2.7. Not to accept for processing any complaints and claims of the Client that do not meet the requirements specified in paragraphs 7.7 to 7.8 of these Regulations.

6.2.8. exercise other rights provided for by these Regulations.

6.3. The Client undertakes to:

6.3.1. inform the Bank in writing about all changes in the information specified in the application no later than 3 (three) working days from the date of their change with the necessary supporting documents.

6.3.2. to perform transactions on Account in accordance with the current legislation of the Kyrgyz Republic, to comply with these Regulations including a set of measures to comply with safety rules when using the RBS.

6.3.3. comply with the legislation of the KR on counteracting terrorist financing and anti-money legalization (laundering) (hereinafter, CTF/AML) and also to provide the Bank with requested information and documents relating to activities of the Client and his/her operations in accordance with the requirements of the legislation of the KR regulating the issues on CTF/LCP. In addition to contracts and primary documents (invoices, waybills, delivery documents, etc.), the Bank is entitled to request copies of financial documents, the Client's statements, the Client's explanations about the economic substance of operations, the source of origin of funds, information about counterparties/payees, and other documents.

6.3.4. pay for the services and commissions of the Bank for remote banking services and account transactions in accordance with the tariffs of the Bank, as well as to pay for the services of other banks involved in the process of performing account transactions by the Client and any other expenses related to Client service and transactions within one banking day from the date of billing by the Bank.

6.3.5. in case of replacement of the mobile phone number provided by the Client to the Bank for the purpose of receiving SMS messages with OTP codes to the Internet Bank, it is mandatory to notify the Bank in writing.

6.3.6. bear other duties provided by these Regulations.

6.4. The Client has the right to:

6.4.1. use the full range of RBS on the terms provided by these Regulations;

6.4.2. receive advice from the Bank on connection and use of RBS;

6.4.3. set and change authorization data for use of RBS on a regular basis;

6.4.4. exercise other rights provided for by these Regulations.

7. Liability of the Parties and dispute resolution

7.1. The Bank shall take all possible measures to resolve the dispute arising within the framework of the RBS use, and shall notify the Client of results.

7.2. Disputes and disagreements arising as a result of the implementation of these Regulations shall be resolved by negotiations between the Client and the Bank. In case of impossibility of dispute resolution in a pre-judicial order the dispute is subject

to consideration in court in the territory of the Kyrgyz Republic according to the legislation of the Kyrgyz Republic.

7.3. If necessary, the Bank may involve various specialists and experts (both employees and non-employees of the Bank) with the necessary experience and knowledge in the relevant field to resolve the dispute.

7.4. The Parties are responsible for non-performance or improper performance of their duties provided for by these Regulations and the legislation of the Kyrgyz Republic.

7.5. The Client is responsible for the device used to connect to the RBS, for using only the licensed software with the latest updates installed, as well as the licensed anti-virus software with up-to-date anti-virus databases on the device used, for losses incurred by the Bank as a result of execution of orders submitted to the Bank on behalf of the Client by an unauthorized person.

7.6. The Client shall be liable for late and/or incomplete notifying the Bank in written about the circumstances relevant for the provision of RBS including changes in the information previously communicated to the Bank. The Client will bear responsibility for possible negative consequences in case of untimely or incomplete notification of the Bank about such circumstances.

7.7. All complaints and claims are sent by the Client to the Bank in writing in accordance with the Bank details specified on the Bank's website: www.keremetbank.kg

7.8. Complaints and claims of the Client related to transaction shall be submitted to the Bank within 30 (thirty) working days from transaction date.

7.9. Results of the Bank's consideration of complaints and claims shall be sent to the Client in writing to the address specified in the application within no more than 30 (thirty) calendar days from the date of receipt of complaint/claim.

7.10. The Client, by accepting these Regulations, expresses his/her unconditional consent that the Bank is not liable:

7.10.1. for errors, delays or inability of the Client to gain access to the RBS system related to the malfunction of the Client's equipment or communication channels, technical means, other resources and services with the help of which the service is performed in the RBS system provided by a third party (Internet access providers, communications, etc.);

7.10.2. for damage to the Client's equipment, for security of the Client's software and personal computer from various viruses and other damages;

7.10.3. for consequences of untimely notification by the Client of the Bank about the loss (theft) of password, mobile phone/SIM card to which mobile phone number is attached, which is communicated by the Client to the Bank in order to receive SMS with OTP, for improperly performed Transactions and attempts of unauthorized access to the Client's Account using the RBS system. Any losses and liability resulting from such actions shall be born by the Client;

7.10.4. for consequences of not notifying by the Client of the Bank about the change of phone number for receiving SMS with OTP, details (including postal address) specified by the Client for receiving information;

7.10.5. for failure to execute the Client's payment orders in the system if order was not provided in full (in incorrect format) and/or included information contrary to the current legislation of the Kyrgyz Republic;

7.10.6. for damage resulting from disclosure of authorization data by the Client, failure to ensure their confidentiality or failure to take measures to keep them secret from third parties, transfer them to third parties regardless of the reasons;

7.10.7. for the Client's losses caused by execution by the Bank of Transactions Orders from unauthorized persons made as a result of access to the RBS system, in cases when such access occurred in the situation which is not

subject or not falling under control from the Bank (compromise of the Client's logins and passwords);

7.10.8. for damages caused by the execution of Transactions Orders from unauthorized persons committed as a result of use by third parties of the Client's authentication data including the illegal methods, disclosure of the Client's authentication data, also caused by information leakage directly from the Client's device, harmful effects of software installed on the Client's device used to access the RBS, phishing, hacking, virus attacks from the Internet;

7.10.9. for Client's losses caused by execution by the Bank of Transaction Orders from unauthorized persons received by the Bank as a result of access and use of the service by third parties if it was not the fault of the Bank;

7.10.10. The Bank is not responsible for inability to provide the service if such occurred due to force majeure circumstances beyond the control of the Bank including but not limited to failures in provision of communication by Internet providers;

7.10.11. for inability to use mobile phone due to damage and/or loss/theft of the SIM-card, for harmful effects of software installed on the Client's mobile phone resulting in compromise of OTP, for damages resulting from unauthorized use by third parties of the Client's OTP;

7.10.12. when information transmitted during the use of RBS including 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 through communication channels used by the Client, as well as in case of unfair performance by the Client of storage conditions and use of means for authentication;

7.10.13. for quality of delivery of SMS to the Client's mobile phone, for delivery and speed of SMS transmission and does not guarantee confidentiality and integrity of information transmitted in form of SMS. The Bank shall not be liable for failures, accidents and overloads in the operation of mobile/movable radiotelephone networks, failures and delays in the operation of mobile radiotelephone operators, problems with the use of mobile/movable radiotelephone by the Client in roaming, i.e. outside the mobile/movable radiotelephone operator's communication network;

7.10.14. in the case of arbitrary or intentional interference of third parties in the private affairs of the Client (including those relating to civil relations between the Client and the Bank) carried out by unfair use by a third party of the means of communication and the Client's contact information communicated to the Bank. The Bank is not responsible for transmission by the Client to third party of mobile phone (SIM card), illegal manufacture by third parties of duplicate SIM card of the Client and use it without knowledge and consent of the Client;

7.10.15. for non-receipt by the Client of information passed by the Bank to the Client in cases stipulated in these Regulations, if contact information submitted to the Bank by the Client became outdated and the Client didn't notice the Bank about it timely in a manner prescribed by the Bank. The Bank shall not be liable for non-fulfillment, untimely or incorrect fulfillment of the Client's orders and/or authentication procedure if this was caused by the Client providing false information, loss of relevance of information previously provided by the Client and used in registration and execution of the Bank's obligations within messaging of OTP or by the Client entering incorrect data. The Client is responsible for correctness and relevance of all information provided to the Bank;

7.10.16. for non-fulfillment of Client's orders using the RBS system if the Client's account was seized or transactions on it were suspended in accordance with the current legislation of the Kyrgyz Republic, as well as in other cases provided for by the legislation of the Kyrgyz Republic;

7.10.17. for losses incurred by the Client through implementation by the Bank of orders prepared by the Client with errors and/or misprints in the information contained in the document fields, as well as in the event of a return of the beneficiary by the Client;

7.10.18. for execution of orders mistakenly transmitted by the Client;

7.10.19. for failure, untimely or improper execution of order if it was caused by the Client's false information, loss of relevance of information previously provided by the Client and used when authorizing or input the wrong data by the Client;

7.11. for non-execution of the Client's order if its execution would lead to violation of requirements of the current legislation of the Kyrgyz Republic, these Regulations, as well as terms of other agreements (contracts) concluded between the Client and the Bank;

8. Force majeure

8.1. The Parties shall not be held liable for violation of term of performance of obligations the cause of which was circumstance of insuperable force (force majeure) which neither Party could not foresee or prevent through reasonable action. Force majeure circumstances include, but are not limited to: natural disasters, fire accident, flood, earthquake, other natural or industrial disasters, epidemics, military actions, coup, state of emergency, revolutions, riots, terrorist acts, civil unrest, actions of the Government, government bodies, National Bank of the Kyrgyz Republic, normative acts entered into force after the date of contract of remote banking services, adoption of the National Bank of the Kyrgyz Republic and/or state authorities of the Kyrgyz Republic decisions resulting in impossibility of performance by the Party of his/her obligations and other circumstances beyond the reasonable control of the Parties.

8.2. The occurrence of force majeure shall entail an increase of the period of performance of the relevant obligations for a period during which such circumstances were in force.

8.3. The proper proof of force majeure will be the documents issued by the authorized state bodies. The Party referring to force majeure circumstances shall provide evidence of force majeure circumstances at the request of other Party.

9. Other conditions

9.1. The Client may be disconnected from the RBS at his/her own request within 5 (five) working days after submitting the relevant written application to point of sale of the Bank.

9.2. In case of disconnection of the Client from the RBS at his/her own request or at the initiative of the Bank (as a result of non-compliance/violation of these Regulations; in cases provided for by law), the Bank deprives the Client of the opportunity to start an authorized work session and it notifies the Client in the appropriate RBS service after an attempt to enter authorization data.

9.3. The Agreement concluded between the Bank and the Client on the terms specified in these Regulations shall be automatically terminated/dissolved upon disconnecting the Client from the RBS. Termination of the remote banking service agreement does not relieve the Parties from liability for its violation which took place before the termination of the agreement.

9.4. In all matters not provided for in these Regulations the Parties shall be guided by the current legislation of the Kyrgyz Republic.

Annex No. 1
to the Regulations on the Provision and Use of Remote Banking Services

Information for the user (Client)

To ensure security in the course of operations within the framework, remote services and the protection of personal data, users must be informed of their duties and responsibilities.

1. When using Internet Banking, the user should:

1) use a secure login and password/personal identification number while not disclosing to unauthorized persons login, password and personal identification number;

- do not store login, password and personal identification number on access devices (personal computer, mobile phone, etc.) or other unprotected media;

- periodically change code, password and personal identification number, not use passwords with low security such as name or date of birth. The password must contain a combination of at least 9 characters: letters (uppercase and lowercase), special characters, and numbers;

2) ensure the confidentiality of personal information by:

- not disclosing personal information (phone or passport number, Bank account number or E-Mail address) to third parties;

3) store information about electronic transactions by:

- regularly checking transaction history and statements to track errors or unauthorized account transactions;

- immediately informing provider, remote/distant service of any unauthorized use of account or transactions;

4) check the correctness and security of the web page by:

- ensuring that the correct web page of Internet Banking and Mobile Banking is used before carrying out any online transactions or providing personal information. It is necessary to beware of fake web pages created for the purpose of fraud;

- It's necessary to ensure the security of the web page by checking for Uniform Resource Locator (URL) which must begin with "https" and status of the Internet browser must show a sign of a secure connection;

- always enter the URL of a web page directly into the Internet browser. Avoid redirects or links to other untrusted pages;

- if possible, use a program that automatically encrypts or encodes the transmitted information in the course of electronic transactions;

5) protect your access device (personal computer, mobile phone, etc.) from unauthorized access and malicious software, while monitoring the regular update of the antivirus program and its constant operation;

6) it is necessary to leave the site where electronic operations are carried out, even if the computer is left unattended for a short time;

- do not forget to log out after performing electronic operations;

7) familiarize yourself with the security policy of the Internet Banking system:

- it is necessary to carefully read the terms of the Internet Banking system regarding payments, transfers, debiting/crediting the account and other terms of banking services;

- it is necessary to read carefully the terms of use or distribution of personal financial information of the Internet Banking system before entering.

2. When using Mobile Banking, user should:

- not disclose to third parties personal identification number (PIN), password, E-Mail password, and other information that may facilitate unauthorized access during remote/distant service on behalf of user;

- periodically change personal identification number used for mobile banking;

- not allow others to use your mobile phone through which the banking operation is carried out;

- immediately inform the servicing Bank/ communications provider/ payment system operator in case of loss or theft of a mobile phone;

- not send personal information especially password or personal identification number through E-Mail, social networks and other means of electronic data exchange;

- immediately inform the service provider if user has any questions regarding the security of Bank account.

Necessary measures to ensure the safe storage of cards, their details, personal identification number and security of other data are defined in the regulatory legal acts of the National Bank.