The list of services and the schedule of service in the Internet Banking system

#	Name of the operation	The time of carrying out the operation
1	Viewing of balances and account activity	24/7
2	Viewing of indebtedness to the Bank	24/7
3	Repayment of debt to the Bank (loan)	8.30-16.30
4	Currency conversion (currency exchange)	8.30-16.30
5	Intrabank transfers (money transfers from the client's own account/ accounts to an account opened in the Bank)	8.30-16.30
6	Clearing payments (money transfers from the client's own account/ accounts to an account opened in another bank in real-time mode)	8.30-11.00
7	Gross payments (money transfers from the client's own account/ accounts to an account opened in another bank)	8.30-15.30
8	Card account management	8.30-16.30
9	International money transfers via the SWIFT system with the cut off time: • Accepting payments in Kazakh tenge with the same day value charge – till 15:00 . • Accepting payments in Russian roubles with the same day value charge – till 15:30. • Accepting payments in US dollars and euros with the same day value charge – till 16:00. • Accepting payments in other currencies with the same day value charge - till 12:00.	After the indicated CUT-off time payments are accepted with the time of performance "next business day"

* Electronic instructions of the Client received by the Bank during the time of carrying out the operation are fulfilled by the Bank on the same business day.

* Electronic instructions of the Client received by the Bank after the specified time of carrying out the operation are fulfilled by the Bank on the next business day.

* Electronic instructions sent by the Client on non-business days are fulfilled by the Bank on the first business day.

* The Bank carried out the final processing and sends the money transfer via the SWIFT system after checking up all the indicated details and provided documents of the clients. The Bank has a right to refuse to make the money transfer if it doesn't receive the required data from the client of if the data/details of the money transfer are inadequate/ incomplete.

GUIDELINES FOR USING INTERNET BANKING

1. The operating mode of Internet Banking:

1.1. There are four modes of access to the Internet Banking system for legal entities:

- View mode – provides access to viewing the balance on the client's own bank account;
- Full mode – provides an opportunity to carry out bank account operations;
- Operator mode – provides an opportunity to create bank account operations;
- Approver mode – provides an opportunity to approve bank account operations created by the operator.

1.2. There are two modes of access to the Internet Banking system for individuals:

- View mode – provides access to viewing the balance on the client's own bank account;
- Full mode – provides an opportunity to carry out bank account operations.

2. Requirements to the work:

2.1. Provide non-disclosure mode in respect of one's own working place for work in the Internet Banking system, in respect of logins and passwords to the operating system of the Client's work place;

2.2. After completing work in the Internet Banking system, it's correct to complete the work using the software button "Exit";

2.3. Disconnect the function of automatic start of removable media in the operating system of the Client's workplace for working in the Internet Banking system;

2.4. Connect the Client's workplace for working in the Internet Banking system to the Internet network only during the work with the Internet Banking system;

2.5. Before entering the personal online area (account), ensure that the protected connection via https established exactly with the official website of the Bank (https://fincabank.kg);

2.6. Ensure the availability of the accounts of the users of the system in the operating system protected by a password on the workplace of the users;

2.7. Not to save password in text files on the computer or on other data storage devices;

2.8. Never, no away, under no circumstances, inform anyone about your password – it's not required for any employees of the Bank and to the technical support service for your connection, maintenance and support of service in in good operating condition;

2.9. Not to use the workplace for connecting to social media in the Internet network, to forums, conferences, chats, telephony services and other websites containing potential malicious software, as well as software for reading e-mail and opening e-mail documents from trustworthy addressees;

2.10. Not to disclose logins and passwords to the third parties, including employees of the Bank (including in the case of appeal of unidentified persons on behalf of the Bank by phone, by e-mail, by a text message (SMS));

2.11. Not to save logins and passwords in the text files on the hard disk of the Client's workplace or on any other electronic data storage devices.

3. Recommendations to follow in the course of work:

3.1. Use the allocated client's workplace, not used by the Client for other purposes, for work with the Internet Banking system;

3.2. Provide functioning of a licensed (not counterfeit) operating system Microsoft Windows XP/2003/Vista/7, Apple Macintosh Mac OS X and later, Linux and its timely updating in accordance with the 10 recommendations of the developer company on the Client's workplace, for the purpose of eliminating the vulnerabilities identified in it, providing an opportunity for someone to get access to confidential information;

3.3. Provide functioning of licensed (not counterfeit) antivirus software and its timely updating in accordance with the recommendations of the developer company on the Client's workplace, in order to prevent infection of the Client's workplace with the malware which is able to provide access to the Internet Banking System to unauthorized third parties;

3.4. Provide functioning of licensed (not counterfeit) software of brandmauer (firewall) on the Client's workplace in the mode of blocking unauthorized remote access to the workplace from the Internet network and from the Client's local network;

3.5. Restrict access to the Client's personal computer and to provide availability of the minimum rights to change configuration of the operating system of the Client's workplace (availability of the administrator's rights is undesirable);

3.6. Not to work in the Internet Banking System in the Internet network using the source of net connection from untrustworthy places (cyber cafes) or using public communication channels (free Wi-Fi etc.);

3.7. Pay attention to any changes and errors of the software in the course of setting up connection in the Internet Banking System or in the course of work of Internet Banking, in the case of any doubts in the correctness of work of Internet Banking System, work shall be immediately stopped and it's necessary to turn to the Bank for the purpose of identification of existence/ absence of unauthorized operations;

3.8. Go to the website https://www.online.finca.kg / only using the reference from the official website of the Bank (www.fincabank.kg);

3.9. In the case if the browser's warning about redirection to another website is displayed in the course of connecting the Internet Banking System, suspend carrying out operations and turn to the Technical Support Service (HelpDesk) of the Bank in order to identify the reason of redirection.

3.10. Inform the authorized employees of the Bank about any attempts to ascertain the password to the Internet Banking System;

3.11. Regularly check up the history of operations and statements for tracking down errors or unauthorized account operations;

3.12. Exit from the website where the electronic operations are carried out, even if the PC is left unattended for a short period of time;

3.13. Remember to log off from the system after the completion of carrying out electronic operations; before carrying out any online operations or providing personal information, it's necessary to ensure that the correct web-page of the Internet Banking System is being used. It's necessary to beware of forged web-pages created for the purpose of fraud;

3.14. Before entering the system, ensure that the web-page is safe, checking up the availability of Uniform Resource Locator (URL) which shall start with "https", and the symbol of protected connection shall appear on the status of the Web browser;

3.15. Non-fulfilment of the requirements and recommendations above by the Client constitute grounds for holding the Client responsible for the contested operations carried out using the Internet Banking System.