Перечень услуг и график обслуживания в системе «Интернет-Банкинг»

№	Наименование операции	Время проведения операции
1	Просмотр остатков и движений по счёту/счетам	24/7
2	Просмотр задолженностей перед Банком	24/7
3	Погашение задолженности перед Банком (кредит)	8.30-16.30
4	Конвертация валют (обмен валют)	8.30-16.30
5	Внутрибанковские переводы (денежные переводы со своего счета/счетов на другой счёт, открытые в Банке)	8.30-16.30
6	Клиринг платежи (денежные переводы со своего счета/счетов на счёт, открытый в другом банке в режиме реального времени)	8.30-11.00
7	Гросс платежи (денежные переводы со своего счета/счетов на счёт, открытый в другом банке)	8.30-15.30

*Электронные распоряжения Клиента, полученные Банком в течение времени проведения операции, исполняются Банком в тот же рабочий день.

* Электронные распоряжения Клиента, полученные Банком после установленного времени проведения операций, исполняются Банком на следующий рабочий день.

* Электронные распоряжения, отправленные Клиентом в нерабочие дни, исполняются Банком в первый рабочий день.

ПРАВИЛА ПОЛЬЗОВАНИЯ ИНТЕРНЕТ БАНКИНГОМ

1. Режимы работы «Интернет Банкинга»:

1.1. в системе Интернет Банкинг для юридических лиц имеются четыре режима доступа в систему:

- Режим просмотр – предоставляет доступ на просмотр остатка по своему банковскому счету;
- Полный режим – предоставляет возможность производить операции по банковскому счету;
- Режим исполнитель – предоставляет возможность создавать операции по банковскому счету;
- Режим авторизатор – предоставляет возможность утверждать операции по банковскому счету, созданные исполнителем.

2. Требования при работе:

2.1. обеспечить режим конфиденциальности в отношении своего рабочего места для работы в системе «Интернет-Банкинг», логинов и паролей к операционной системе рабочего места Клиента;

2.2. после окончания работы в системе «Интернет-Банкинг» корректно завершать работу с использованием программной кнопки «Выход»;

2.3. отключить в операционной системе рабочего места Клиента для работы в системе «Интернет - Банкинг» функцию автозапуска съемных носителей информации;

2.4. подключать рабочее место Клиента для работы в системе «Интернет-Банкинг» к сети Интернет только во время работ с системой «Интернет-Банкинг»;

2.5. перед входом в личный кабинет убедится, что защищенное соединение по протоколу https установлено именно с официальным сайтом Банка (https://finca.kg)

2.6. обеспечить у пользователей системы на рабочем месте наличие учетной записи в операционной системе, защищенной паролем;

2.7. не сохранять пароль в текстовых файлах на компьютере, либо на других носителях информации;

2.8. никогда ни при каких обстоятельствах не сообщать никому пароль – он не требуется сотрудникам Банка и службе технической поддержки для вашего подключения, обслуживания и поддержки сервиса в работоспособном состоянии;

2.9. не использовать рабочее место для подключения к социальным сетям в сети Интернет, к форумам, конференциям, чатам, телефонным сервисам и иным сайтам, содержащим потенциальные вредоносные программы, а также для чтения почты и открытие почтовых документов от адресатов, незаслуживающих доверия;

2.10. не раскрывать логины и пароли третьим лицам, включая сотрудников Банка (в том числе при обращении неустановленных лиц от имени Банка по телефону, электронной почте, через SMS);

2.11. не сохранять логины и пароли в текстовых файлах на жестком диске рабочего места Клиента, либо на других электронных носителях информации.

3. Рекомендации при работе:

3.1. использовать для работы с системой «Интернет-Банкинг» выделенное рабочее место Клиента, не используемое Клиентом в других целях;

3.2. обеспечить функционирование на рабочем месте Клиента лицензионной (не контрафактной) операционной системы Microsoft Windows XP/2003/Vista/7, Apple Macintosh Mac OS X или старше, Linux и ее своевременное обновление согласно 10

рекомендациям компании-разработчика в целях устранения, выявленных в ней уязвимостей, позволяющих получить доступ к конфиденциальной информации;

3.3. обеспечить функционирование на рабочем месте Клиента лицензионного (не контрафактного) антивирусного программного обеспечения и его своевременное обновление согласно рекомендациям компании-разработчика, в целях недопущения заражения рабочего места Клиента вредоносным программным обеспечением, способным предоставить доступ к Системе «Интернет Банк» Клиента неуполномоченным третьим лицам;

3.4. обеспечить функционирование на рабочем месте Клиента лицензионного (не контрафактного) программного обеспечения «брандмауэр (firewall)» в режиме блокирования несанкционированного удаленного доступа к рабочему месту из сети Интернет и локальной сети Клиента;

3.5. ограничить доступ к персональному компьютеру Клиента и обеспечить наличие минимальных прав для изменения конфигурации операционной системы рабочего места Клиента (наличие прав администратора нежелательно);

3.6. не работать в системе «Интернет-Банкинг» в сети Интернет, используя источник подключения из мест, не заслуживающих доверия (интернет-кафе), или используя общественные каналы связи (бесплатный Wi-Fi и т.п.);

3.7. обращать внимание на любые изменения и ошибки программного обеспечения во время установления соединения в системе «Интернет-Банкинг» Банка или в работе интернет банкинга, при возникновении любых сомнений в правильности работы интернет банкинга незамедлительно прекратить работу и обратится в Банк в целях установления отсутствия/наличия несанкционированные операций;

3.8. переходить на https://www.online.finca.kg / только по ссылке с официального сайта Банка (www.finca.kg);

3.9. в случае появления предупреждений браузера о перенаправлении на другой сайт при подключении к системе «Интернет-Банкинг», отложить совершение операций и обратиться в службу технической поддержки Банка в целях установления причине перенаправления.

3.10. сообщать уполномоченным сотрудникам Банка о любых попытках узнать пароль в систему «Интернет-Банкинг»;

3.11. регулярно проверять историю операций и выписки для отслеживания ошибок или неавторизированных операций по счету;

3.12. не покидать сайт, где осуществляются электронные операции, даже если персональный компьютер оставлен без присмотра на короткий срок;

3.13. не забывать выходить из системы после осуществления электронных операций; перед осуществлением любых онлайн операций или предоставление личной информации должен убедиться, что используется правильная веб-страница системы «Интернет-Банкинг». Необходимо остерегаться фальшивых веб-страниц, созданных в целях мошенничества;

3.14. перед входом в систему, убедиться в безопасности веб-страницы, проверив наличие Унифицированных Указателей Ресурсов (URL), которые должны начинаться с «https», а на статусе интернет-браузера должен появиться знак защищенного соединения;

3.15. Не исполнение вышеперечисленных требовании и рекомендаций Клиентом, будет являться основанием для возложения ответственности за оспариваемые операции посредством системы «Интернет-Банкинг» на Клиента.