«Bank RBK» АҚ Заңды тұлғалар, жеке кәсіпкерлер,
шаруа (фермер) қожалықтары, жеке нотариустар, адвокаттар,
жеке сот орындаушылары, кәсіби медиаторлар үшін
«Интернет-Клиент» жүйесінде қашықтан банктік
қызмет көрсету шартының жалпы талаптарына
1-қосымша
Приложение 1
к Общим условиям договора дистанционного банковского
обслуживания в системе «Интернет-Клиент» для юридических лиц,
индивидуальных предпринимателей, крестьянских (фермерских) хозяйств,
частных нотариусов, адвокатов, частных судебных исполнителей,
профессиональных медиаторов в АО «Bank RBK»
Appendix 1
to the General Terms and Conditions of the Remote Banking Services Agreement in the "Internet-Customer" system for Legal Entities,
Individual Entrepreneurs, Peasant (Farm) Enterprises,
Private Notaries, Lawyers, Private Court Bailiffs, and Professional Mediators
in "Bank RBK" JSC

Жүйедегі жұмыс кезіндегі қауіпсіздік рәсімдері

1. Банк Клиенттерге шотты (-тарды) қашықтан басқару және интернет желісі арқылы банктік қызмет көрсету қосымшалары үшін пайдаланылатын стандартты салалық шифрлау болып табылатын интернет арқылы дербес банктік қызмет көрсетудің барлық қосымшаларымен 256-bit SSL (Secure Sockets Layer-қауіпсіз қосылыстар хаттамасы) хаттамасы көмегімен ақпаратты шифрлеу тетіктеріне негізделген қауіпсіздіктің кепілдік деңгейі бар жалпы қолжетімді Интернет желісі арқылы Электрондық банктік қызметтерді алу, сондай-ақ Қашықтан қызмет көрсету мүмкіндігін ұсынады.

2. Қауіпсіздіктің кепілді деңгейін қамтамасыз ету және берілетін және алынатын ақпараттың құпиялылығын қамтамасыз ету мақсатында жүйеде TLS256 bit (Transport Layer Security — көлік деңгейінің қауіпсіздігі) шифрлауы пайдаланылады. Шифрлау клиенттің деректерін Интернет желісі арқылы жіберер алдында шифрленген кодқа жүйеде түрлендіреді және Банктің компьютерлік жүйесі мен клиенттің интернет-браузері арасындағы аралықта Клиент ақпаратының құпиялылығын қамтамасыз етеді.

3. Ақпаратты қорғауды қамтамасыз ету бойынша барлық рәсімдер клиенттің пайдаланушылық дербес компьютерлерінде, интернет желісінде және жүйе серверлерінде орындалады.

Процедуры безопасности при работе в Системе

1. Банк предоставляет Клиентам возможность удаленного управления Счетом (-ами) и получения Электронных банковских услуг, а также Дистанционного обслуживания посредством Системы через общедоступную сеть интернет с гарантированным уровнем безопасности, основанным на механизмах шифрования информации с помощью протокола 256-bit SSL (Secure Sockets Layer - протокол безопасных соединений) со всеми приложениями персонального банковского обслуживания через интернет, которое является стандартным отраслевым шифрованием, используемым для приложений банковского обслуживания через сеть интернет.

2. В целях обеспечения гарантированного уровня безопасности и обеспечения конфиденциальности передаваемой и получаемой информации в Системе используется шифрование TLS256 bit (Transport Layer Security — безопасность транспортного уровня). Шифрование преобразует данные Клиента в Системе в зашифрованный код перед их отправкой через сеть интернет и обеспечивает конфиденциальность информации Клиента на пути между компьютерной системой Банка и интернет-браузером Клиента.

3. Все процедуры по обеспечению защиты информации выполняются на пользовательских персональных компьютерах Клиента, в сети интернет и на серверах Системы. Клиент должен обеспечить

Security procedures when operated at System

1. The Bank provides the Customers with an opportunity to manage the Account(s) remotely and to receive Electronic Banking Services, as well as Remote Servicing using the System via Internet with a guaranteed security level based on 256-bit SSL protocol encryption mechanisms (Secure Sockets Layer) with all Internet personal banking applications, which is standard industry encryption for Internet banking applications.

2. With a view to ensuring a guaranteed level of security and ensuring the confidentiality of the transmitted and received information, the System uses TLS256 bit encryption (Transport Layer Security). Encryption converts the Customer's data in the System into an encrypted code before sending it via the Internet and ensures the confidentiality of the Customer's information on the way between the Bank's computer system and the Customer's Internet browser.

3. All data protecting procedures are performed on the Customer's personal computers, on the Internet and on the System's servers. The Customer must ensure the availability of a modern browser with 256 bit encryption support.

Клиент 256 bit шифрлауды қолдайтын қазіргі заманғы браузердің болуын қамтамасыз етуі тиіс.

4. Жүйеде компьютерлік жүйелерге әлеуетті қауіпті ақпараттың енуін бұғаттау және жүйеге рұқсатсыз кіруді болдырмау үшін желіаралық экрандар (firewall/Brandmauer) қолданылады. Желіаралық экрандардың бағдарламалық жасақтамасы офистік және үй компьютерлерінде рұқсатсыз кіру мен вирустардан қорғау ретінде орнатылады.

5. Клиенттің компьютерін және Клиенттің жүйеге қосылған шоттары туралы ақпаратты қорғау мақсатында Банк Банкпен байланысты орнатуды тексеру үшін сандық сертификаттарды пайдаланады. Банктің интернет-ресурсында жүйеде аутентификация және динамикалық сәйкестендіру кезінде Клиенттің браузері сандық сертификаттар арқылы өзінің сәйкестендіру ақпаратын Банктің интернет-ресурсын растауды сұратады. Клиенттің браузері сертификатты тексере алады және егер осы интернет-ресурсы Банкке тиесілі емес болса Клиентке ескерте алады. Клиент осы тексерістің орын алғандығына көз жеткізуге міндетті.

6. Банкте тіркеу кезінде алынған логин және дербестендірілмеген (стандартты) пароль бойынша жүйеге алғашқы кіру жүзеге асырылған кезде жүйе осындай парольді міндетті түрде ауыстыруды және Клиентті - ЭЦҚ және (немесе) ОТР таңдауға сәйкестендірудің қосымша факторын сұратады. Жүйеде дербестендірілмеген (стандартты) құпия сөзді ауыстырусыз операциялар жасау мүмкін емес.

7. Келесі ең төменгі талаптарды қанағаттандыратын парольдерді қою ұсынылады:

1) парольде пайдаланушының есептік жазбасының аты немесе оның қандай да бір бөлігі, туған күні, тек сандар немесе жай сөздер қамтылмайды;

2) Парольдің ұзындығы кемінде 8 (сегіз) символдан тұруы тиіс;

наличие современного браузера с поддержкой шифрования 256 bit.

4. В Системе используются межсетевые экраны (firewall/Brandmauer) для блокировки проникновения в компьютерные системы потенциально опасной информации и предотвращения несанкционированного доступа в Систему. Программное обеспечение межсетевых экранов может быть установлено на офисных и домашних компьютерах в качестве защиты от несанкционированного доступа и вирусов.

5. В целях защиты компьютера Клиента и информации о подключенных Счетах Клиента к Системе Банк использует цифровые сертификаты для проверки установления связи с Банком. При Аутентификации и Динамической идентификации в Системе на интернет-ресурсе Банка браузер Клиента запрашивает подтверждение интернет-ресурса Банка своей идентификационной информации посредством цифровых сертификатов. Браузер Клиента может проверить сертификат и предупредить Клиента, если данный интернет-ресурс не принадлежит Банку. Клиент обязан удостовериться в том, что данная проверка имела место быть.

6. При осуществлении первого входа в Систему по Логину и неперсонифицированному (стандартному) паролю, полученным при регистрации в Банке, Система запрашивает обязательную смену такого пароля и дополнительный фактор Идентификации на выбор Клиента - ЭЦП и (или) ОТР. Выполнение операций в Системе без смены неперсонифицированного (стандартного) пароля невозможно.

7. Рекомендуется задавать Пароли, удовлетворяющие следующим минимальным требованиям:

1) пароль не может содержать имя учетной записи Пользователя или какую-либо его часть, дату рождения, только цифры или простые слова;

2) длина Пароля должна состоять не менее чем из 8 (восьми) символов;

4. The System uses inter-network screens (firewall / Brandmauer) to block the penetration of potentially dangerous information into computer systems and prevent unauthorized access to the System. Inter-network screens software can be installed on office and home computers as protection against unauthorized access and viruses.

5. With the aim of protecting the Customer’s computer and information about the connected Customer Accounts to the System, the Bank uses digital certificates to verify that it has established communications with the Bank. During authentication and Dynamic identification in the System on the Bank’s Internet resource, the Customer’s browser requests confirmation of the Bank’s Internet resource of its information identification by digital certificates. The Customer's browser can verify the certificate and notify the Customer if this Internet resource is not owned by the Bank. The Customer is obliged to ensure that this verification took place.

6. At primary log in to the System using a Login and a non-personalized (standard) password obtained during registration with the Bank, the System requests a mandatory change of such a password and an additional Identification factor to choose the Customer - Electronic digital signature and (or) OTP. Carrying out operations in the System without changing a non-personalized (standard) password are impossible.

7. It is recommended to set passwords that meet the following minimum requirements:

1) the password can not contain the name of the User account or any part of it, date of birth, only numbers or simple words;

2) the password length must consist of at least eight (8) symbols;

3) парольде ағылшын алфавитінің бас және кіші әріптерінің, сандар мен ерекше символдардың (мысалы:!,$,#, % және т. б.) тіркесі болуы тиіс.

8. Кілтті тасығышты және (немесе) OTP пайдалана отырып, электрондық құжатты Аутентификациялағаннан кейін редакциялау, сондай-ақ егер Клиент жүйеде электрондық құжатты аутентификациялауды дербес жоймаса, электрондық құжат аутентификациясын өзгерту мүмкін емес. Электрондық құжаттың дұрыс мазмұны үшін барлық жауапкершілік Клиентке жүктеледі.

9. Электрондық құжатты Банкке жіберу кезінде жүйе, егер осы электрондық құжатты Клиент бұрын куәландырмаған жағдайда, негізгі тасығышты және (немесе) OTP-Token пайдалана отырып, қайта аутентификациялауды талап ете алады.

10. Пайдаланушы жүйеге кіру үшін парольді бірнеше рет (үш әрекет) қате енгізген жағдайда, жүйеде пайдаланушының есептік жазбасын банк автоматты түрде бұғаттайды. Пайдаланушыға есептік жазбаны бұғаттауды Банк банкке жеке өтініш берген кезде Есептік жазбаны бұғаттаудан шығару туралы Клиенттің жазбаша өтініші негізінде жүзеге асырады. Қажет болған жағдайда, парольді ауыстыру жүйе арқылы және парольді ауыстыру үшін SMS алу арқылы немесе дербестендірілмеген (стандартты) парольді алу және кейіннен парольді ауыстыру арқылы жүйеге кіруді жүзеге асыру үшін банкке жүгіну арқылы жүзеге асырылады.

Клиенттің логинді, парольді, ЭЦҚ және (немесе) OTP дұрыс енгізбеуі Банктің Электрондық банктік қызметті, Қашықтан қызмет көрсетуді ұсынбауы үшін негіз болып табылады.

11. Қауіпсіздік мақсатында жүйеде пайдаланушының белсенді әрекеті ұзақ (15 минуттан артық) болмаған жағдайда жүйеде Клиенттің ағымдағы сессиясын өшіру функциясы қарастырылған. Жүйеге қайта кіру үшін пайдаланушы кіру рәсімін қайта жүзеге асыруы қажет. Бұл ретте

3) в Пароле должно присутствовать сочетание прописных и строчных букв английского алфавита, цифр и специфичных символов (например: !, $, #, % и т.п.).

8. После Аутентификации Электронного документа с использованием Ключевого носителя и (или) OTP редактирование, а также изменение в содержании Электронного документа невозможно, если только Клиент самостоятельно не отменит Аутентификацию Электронного документа в Системе. Вся ответственность за правильное содержание Электронного документа возлагается на Клиента.

9. При отправке Электронного документа в Банк Система может потребовать повторной Аутентификации с использованием Ключевого носителя и (или) OTP-Token в случаях, если данный Электронный документ не был удостоверен Клиентом ранее.

10. В случае неоднократного (более трех попыток) неверного введения Пользователем Пароля для доступа в Систему, учетная запись Пользователя в Системе автоматически блокируется Банком. Разблокировка учетной записи Пользователю осуществляется Банком на основании письменного заявления Клиента о разблокировке учетной записи при личном обращении в Банк. При необходимости, смена Пароля осуществляется посредством Системы и получения SMS для смены Пароля, либо путем обращения в Банк для получения нового неперсонифицированного (стандартного) пароля и осуществления входа в Систему с последующей сменой Пароля.

Неверное введение Клиентом Логина, Пароля, ЭЦП и (или) OTP является основанием для не предоставления Банком Электронной банковской услуги, Дистанционного обслуживания.

11. В целях безопасности в Системе предусмотрена функция отключения текущей сессии Клиента в Системе в случае продолжительного (более 15 минут) отсутствия активных действий Пользователя в Системе. Для повторного доступа в Систему Пользователю необходимо заново осуществить

3) password must contain a combination of capital and lowercase letters of the English alphabet, numbers and specific symbols (for example: !, $, #, %, etc.).

8. After the Electronic document Authentication using the Key carrier and (or) OTP, editing, as well as a change in the content of the Electronic document is impossible, unless the Customer cancels the Authentication of the Electronic document in the System. All responsibility for the correct content of the Electronic document rests with the Customer.

9. When sending the Electronic Document to the Bank, the System may require repeated Authentication using the key carrier and (or) OTP-Token in cases where this Electronic document has not been previously certified by the Customer.

10. In the event of repeated (more than three efforts) incorrect password introduction by the User, the User’s account in the System is automatically blocked by the Bank. The User’s account is unblocked on the basis of a the Customer written request on unblocking the User’s account, that is carried by the Customer personal appeal to the Bank. If necessary, the password change is carried out through the System and receiving an SMS to change the password, or by contacting the Bank to obtain a new non-personalized (standard) password and enter the System with the following password change.

The incorrect introduction of the login, Password, Electronic digital signature and (or) OTP by the Customer is a reason for the Bank not to provide the Electronic banking service, Remote servicing.

11. For reasons of safety, the System provides the function of disconnecting the current Customer session in the System in case of a prolonged (more than 15 minutes) absence of active actions by the User in the System. To repeated access the System, the User has to re-perform the login procedure. In these circumstances, it is prohibited to

ағымдағы сессиямен жұмыс орнын пайдаланушы болмаған кезде қалдыруға тыйым салынады.

12. Жүйеде жұмыс істеу кезінде қауіпсіздіктің кепілді деңгейін қамтамасыз ету мақсатында Клиент/пайдаланушы (-лар) өзінің жұмыс орнында қауіпсіздіктің тиісті деңгейін қамтамасыз етуі қажет, соның ішінде, бірақ олармен шектелмей:

1) жүйеге кірген кезде Логин мен парольді, ЭЦҚ және (немесе) OTP енгізу. Банк ешқандай басқа ақпарат сұрамайды;

2) ЭЦҚ және (немесе) OTP негізгі тасымалдаушысына қол жеткізу үшін паролін қолмен енгізу, осылайша Клиентті зиянкестер мен киберқылмыскерлердің алаяқтық әрекеттерінен қорғайтын операциялардың анықтығын растайды.

3) қазіргі заманғы операциялық жүйесі және шектеулі физикалық қолжетімділігі бар жеке компьютерді тек Жүйедегі жұмыс үшін ғана пайдалану, басқа да іс-әрекеттер осы компьютерде жүзеге асырылмауы тиіс, атап айтқанда, басқа бағдарламалармен, электрондық поштамен, интернеттегі сайттарға кіру тәрізді жұмыс;

4) ЭЦҚ кілттерін тек Кілттік тасығышта қауіпсіз сақтауды жүзеге асыруға міндетті. Негізгі тасымалдаушыны жұмыс орнына тек жүйемен жұмыс істеу кезінде ғана орнатуға жол беріледі;

5) жүйеде жұмыс істеген кезде (бірінші және екінші қол қою) ЭЦҚ бірнеше кілттерін пайдаланған жағдайда ЭЦҚ осы кілттерін бір кілтті тасымалдаушыға көшірмеу, сондай-ақ бір мезгілде вирустардың болуына тексерілмеген, иеліктен шығарылатын ақпарат жеткізгіштерін компьютерге қоспау;

6) жүйеде жұмыс істеу үшін қалыптастырылған жеке логинді және кез келген парольдерді, кілтті тасығышты, ЭЦҚ, OTP-Token және (немесе) OTP кілттерін үшінші тұлғаларға (банк қызметкерлерін және клиенттің қызметкерлерін немесе олардың туыстарын қоса алғанда) жария етуге/беруге жол бермеуді қамтамасыз етуге, оларды кез келген үшінші тұлғалар үшін қол жетімсіз, олардың сақталуы мен

процедуру входа. При этом, запрещается оставление рабочего места с текущей сессией в отсутствие Пользователя.

12. В целях обеспечения гарантированного уровня безопасности при работе в Системе Клиенту/Пользователю(-ям) необходимо на своем рабочем месте обеспечивать должный уровень безопасности, включая, но не ограничиваясь:

1) при входе в Систему вводить Логин и Пароль, ЭЦП и (или) OTP. Никакой другой информации Банк не запрашивает;

2) вручную вводить Пароль для доступа к Ключевому носителю ЭЦП и (или) OTP, тем самым подтверждая валидность операций, что защищает Клиента от мошеннических действий злоумышленников и киберпреступников;

3) использовать отдельный компьютер с современной операционной системой и ограниченным физическим доступом, исключительно для работы в Системе, другие действия на этом компьютере осуществляться не должны, а именно, такие как работа с другими программами, электронной почтой, посещение сайтов в интернете;

4) осуществлять безопасное хранение Ключей ЭЦП только на Ключевом носителе. Установка Ключевого носителя на рабочее место допускается исключительно на время работы с Системой;

5) в случае использования нескольких Ключей ЭЦП при работе в Системе (первой и второй подписи) не переносить эти Ключи ЭЦП на один Ключевой носитель, а также не подключать одновременно иные, не проверенные на наличие вирусов, отчуждаемые носители информации к компьютеру;

6) обеспечивать недопущение разглашения/ передачи личного Логина и любого из Паролей, сформированных для работы в Системе, Ключевого носителя, Ключей ЭЦП, OTP-Token и (или) OTP, третьим лицам (включая работников Банка и работников Клиента или их родственников), хранить их в недоступном для любых третьих лиц месте, гарантирующем их сохранность и целостность.

leave the workplace with the current session in the User absence.

12. With a view to ensuring a guaranteed level of security when working in the System, the Customer / User(s) need to ensure an adequate level of security at their workplace, including but not limited to:

1) enter the Login and Password, Electronic digital signature and (or) OTP when entering the System. The Bank does not request any other information;

2) enter by hand the Password for access to the Key carrier and (or) OTP, thereby confirming the validity of the operations, which protects the Customer from malefactor frauds and cybercrooks;

3) use a individual computer with a modern operating system and limited physical access, exclusively for work in the System, other actions on this computer should not be performed, namely, such as working with other programs, e-mail, visiting websites on the Internet;

4) carry out the safe storage of Electronic digital signature keys only on the Key carrier. The installation of the Key carrier on the workplace is allowed only for the period of work with the System;

5) in case of using several Electronic digital signature keys when working in the System (first and second signatures), do not transfer these Electronic digital signature keys to one key carrier, and also do not connect simultaneously other, not verified for viruses, alienable information carriers to the computer;

6) to prevent the disclosure / transfer of personal Login and any of the Passwords created for work in the System, Key carrier, Electronic digital signature keys, OTP-Token and (or) OTP to the third parties (including Bank employees and employees of the Customer or their relatives), to keep them in a inaccessible place to any third parties, guaranteeing their safety and integrity. Transfer of the Key carrier to Bank employees is allowed only in

тұтастығына кепілдік беретін жерде сақтауға міндетті. Кілтті тасымалдаушыны банк қызметкерлеріне беруге ЭЦҚ кілттері мен тіркеу куәлігі жаңартылған жағдайда ғана жол беріледі;

7) лицензиялық, уақтылы автоматты түрде жаңартылып отыратын вирусқа қарсы бағдарламалық жасақтаманы міндетті түрде пайдалануды қамтамасыз етуге міндетті. Вирустардың әрекеті пайдаланушының сәйкестендіру ақпаратын ұстап алуға және оны зиянкестерге беруге бағытталуы мүмкін;

8) қосымша қауіпсіздікті қамтамасыз ету мақсатында пайдаланушы құпия сөзді енгізгенде «Виртуалды пернетақтаны» пайдалана алады;

9) Интернет байланысын орнататын бағдарламаларда, компьютерде мәтіндік файлдарда немесе басқа да электрондық ақпарат тасығыштарда Парольді (-дерді) ешқашан сақтамауға, себебі оны ұрлау және ымыраласу қаупі бар;

10) ЭЦҚ кілттерін олардың қолданылу мерзімі аяқталғанға дейін жаңартуды жүргізуге міндетті. Бұдан басқа, жүйеге рұқсаты бар адамдарды, сондай-ақ ЭЦҚ кілттерін алуға сенімхаттарға қол қою құқығы бар басшыларды жұмыстан босатудың және (немесе) ауыстырудың барлық жағдайларында және олардың ымыраға келуіне күдік болған жағдайда ЭЦҚ кілттерін жаңартуды жүргізу қажет;

11) компьютер жұмысында іркіліс немесе жүйемен жұмыс істеу кезінде немесе сеанстан кейін бірден бұзылған жағдайда (операциялық жүйенің жүктелуі, қатты дискінің және т. б. істен шығуы), кілтті тасымалдаушыны бірден шығарып, компьютерді өшіріп, сондай-ақ банкке барып, сіздің атыңыздан санкцияланбаған операциялар жүргізілмегеніне көз жеткізу керек;

12) жүйенің дұрыс жұмыс істеуіне кез келген күмән туындаған жағдайда дереу банкке жүгіну;

Передача Ключевого носителя работникам Банка допускается только в случае обновления Ключей ЭЦП и Регистрационного свидетельства;

7) обеспечивать обязательное использование лицензионного, своевременно автоматически обновляющегося антивирусного программного обеспечения. Действие вирусов может быть направлено на перехват идентификационной информации Пользователя и передачи ее злоумышленникам;

8) в целях обеспечения дополнительной безопасности Пользователь при вводе Пароля может использовать «Виртуальную клавиатуру», исключая тем самым возможность перехвата вводимых символов;

9) никогда не сохранять Пароль(-и) в программах, устанавливающих интернет-соединение, в текстовых файлах на компьютере либо на других электронных носителях информации, так как при этом существует риск его кражи и Компрометации;

10) производить обновление Ключей ЭЦП до истечения срока их действия. Кроме того, необходимо проводить обновление Ключей ЭЦП во всех случаях увольнения и (или) смены лиц, имеющих доступ в Систему, а также руководителей с правом подписи доверенностей на получение Ключей ЭЦП, и в случае подозрения на их Компрометацию;

11) в случае сбоев в работе компьютера или его поломки во время работы с Системой или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска и т.п.), следует немедленно извлечь Ключевой носитель и выключить компьютер, а также обратиться в Банк и убедиться, что от Вашего имени не производились несанкционированные операции;

12) при возникновении любых сомнений в правильности функционирования Системы незамедлительно обратиться в Банк;

case of updating the electronic digital signature keys and the registration certificate;

7) ensure the mandatory use of licensed, timely, automatically updated anti-virus software. The effect of viruses may be focused on intercepting the User identification information and transmitting it to attackers;

8) with a view to ensuring additional security, the User may use the “Virtual Keyboard” when entering the password, thereby eliminating the possibility of intercepting input symbols;

9) never save the Password(s) in programs that establish an Internet connection, in text files on a computer or on other electronic media, as there is a risk of its being stolen and compromised;

10) update the Electronic digital signature keys before their expiration date. Furthermore, it is necessary to update the Electronic digital signature keys in all cases of dismissal and (or) change of persons who have access to the System, as well as managers with the right to sign powers of attorney to receive Electronic digital signature keys, and in case of suspicion of their compromising;

11) in case of a computer malfunction or its breakdown during operation in the System or immediately after the session (problems with the operating system loading, hard disk failure, etc.), you should immediately remove the key carrier and turn off the computer, and also address to the Bank and make sure that no unauthorized operations were performed on your behalf;

12) in case of any doubts about the correct functioning of the System, immediately address to the Bank;

13) жүйені қосқан кезде браузердің сізді басқа сайтқа қайта бағыттау туралы ескертулері пайда болған жағдайда операциялар жасауды кейінге қалдыру және Банк пайдаланушыларының қолдау тобына жүгіну;

14) жұмыс аяқталғаннан кейін жүйе терезесін «Шығу» батырмасының көмегімен жабу және жүйеде ағымдағы сессиялары бар компьютерді ешқашан қараусыз қалдырмау қажет.

13. Даулы жағдайларды талдауды жүзеге асыру үшін Банк Клиент пен Банк жіберген/қабылдаған барлық электрондық құжаттардың мұрағатын жүргізуді қамтамасыз етеді. Жүйеде пайдаланушылардың барлық әрекеттері жүйемен қалыптастырылған электрондық журналдарға жазылады.

14. Клиент жүйені, негізгі тасығышты және (немесе) OTP-Token, сондай-ақ оның компьютерлік жүйелерінде сақталатын ақпаратты орнату, қолдау және пайдалану қауіпсіздігін ұйымдастыруға тұрақты бақылау жасау, атап айтқанда, жүйеге кіру үшін парольдерді бақылау, сондай-ақ осы тармақта аталған міндеттерді ҚБҚЖ жалпы талаптарын орындамау себебі бойынша теріс салдарлар үшін толық жауапкершілікті өзіне алады.

15. Клиент Клиенттің барлық пайдаланушылары мен уәкілетті тұлғалары қауіпсіздік рәсімдерімен танысқанын және оларды орындайтын растайды.

16. Клиент Банкті барлық талап-арыздардан және сот талқылауларынан қорғауға, Банктің ҚБҚЖ жалпы талаптарына сәйкес Клиенттің өз міндеттемелерін орындамауы немесе тиісінше орындамауы нәтижесінде Банк ұшырауы мүмкін кез келген түрдегі шығындарды, шығыстар мен залалды өтеуге келіседі.

13) в случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении Системы отложить совершение операций и обратиться в Группу поддержки пользователей Банка;

14) после окончания работы необходимо закрывать окно Системы с помощью кнопки «Выход» и никогда не оставлять компьютер с текущей сессией в Системе без присмотра.

13. Для осуществления анализа спорных ситуаций, Банком обеспечивается ведение архива всех отправленных/принятых Пользователем Клиента и Банком Электронных документов. Все действия Пользователей в Системе записываются в электронные журналы, сформированные Системой.

14. Клиент берет на себя полную ответственность за установку, поддержание и регулярный контроль за организацией безопасности доступа и использования Системы, Ключевого носителя и (или) OTP-Token, а также информации, хранимой в его компьютерных системах, и, в частности, контроль за Паролями для входа в Систему, а также за негативные последствия по причине невыполнения перечисленных в настоящем пункте Общих условий СДБО обязанностей.

15. Клиент подтверждает, что все Пользователи и Уполномоченные лица Клиента ознакомлены с Процедурами безопасности и будут исполнять их.

16. Клиент соглашается оградить Банк от всех исков и судебных разбирательств, возместить Банку издержки, убытки и ущерб любого типа, которым Банк может быть подвержен в результате неисполнения или ненадлежащего исполнения Клиентом своих обязательств согласно Общих условий СДБО.

13) in case of browser warnings about redirecting you to another site when connecting to the System, lay over transactions and address to the Bank's User Support Group;

14) It is necessary to close the System window using the “Exit” button after work and never leave the computer with the current session in the System unkept.

13. For the analysis of disputable situations, the Bank ensures the maintenance of an archive of all sent / received Electronic documents by the User of the Customer and the Bank. All actions of Users in the System are recorded in electronic journals generated by the System.

14. The Customer assumes full responsibility for the installation, maintenance and regular control over the organization of access security and use of the System, Key carrier and (or) OTP-Token, as well as information stored in computer systems, and, in particular, control of Passwords for the System assess, and for negative consequences due to non-fulfilment of the duties specified in this clause of the RBSS General Terms and Conditions.

15. The Customer confirms that all Users and authorized persons of the Customer are familiar with the Security procedures and will comply with them.

16. The Customer agrees to protect the Bank from all claims and legal proceedings, to indemnify the Bank for costs, losses and damages of any type to which the Bank may be exposed as a result of non-fulfilment or improper fulfilment of its obligations by the Customer according to the RBSS General Terms and Conditions.