Евразийский Банк

20___ жылғы _____ №___
ағымдағы банктік шот шартына
№ _қосымша келісім
(заңды тұлғалар, жеке кәсіпкерлер, шаруа немесе фермер қожалықтары, жеке нотариустер (жалпы шаруашылық мақсаттар), жеке сот орындаушылар (жалпы шаруашылық мақсаттар) және адвокаттар үшін)

_____ қ. 20__ ж.«___»_____

"Еуразиялық банк" АҚ, бұдан әрі "Банк" деп аталады,
_____
_
_____негізі
нде әрекет ететін
_____
__
арқылы бір жағынан және
_____
_____
_____ бұдан әрі «Клиент» деп аталады,
_____
_____
негізінде әрекет ететін
_____
_____
арқылы екінші жағынан, бірлесіп Тараптар деп аталады, 20___ жылғы _____ №___ ағымдағы банктік шот шартына (бұдан әрі – Шот шарты) төмендегі туралы осы №_____ қосымша келісімді (бұдан әрі – Келісім) жасады:

1. Қосымшада пайдланылатын терминдер

1.1. Қашықтан банктік қызмет көрсету жүйесі (бұдан әрі - ҚБҚ), Клиентке Интернет желісі арқылы қол жеткізілетін Банктің web-сайты арқылы Клиент пен Банк арасында құжаттарды электрондық түрде (бұдан әрі - электрондық құжаттар) алмастыру арқылы өзінің банктік шоттарын басқару мүмкіндігін беретін жүйе.

1.2. Тіркеу куәлігі - электронды сандық қолдың Қазақстан Республикасының 2003 жылғы 7 қаңтардағы № 370-II "Электрондық құжат және электрондық сандық қол туралы" Заңында белгіленген талаптарға сәйкестігін растау үшін Куәландырушы орталық беретін қағаздық тасымалдағыштағы құжат немесе электрондық

Евразийский Банк

Дополнительное соглашение №__
к Договору текущего банковского счета
№_____ от _____ 20___ года

(для юридических лиц, индивидуальных предпринимателей, крестьянских или фермерских хозяйств, частных нотариусов (общехозяйственные цели), частных судебных исполнителей (общехозяйственные цели) и адвокатов)

г. _____ «___»_____ 20__г.

АО «Евразийский Банк», именуемый в дальнейшем Банк, в лице_____
_____, действующего на основании _____, с одной стороны и _____
_____, именуемое в дальнейшем Клиент, в лице_____

_____
_____, действующего (ей) на основании_____
_____
_____,
с другой стороны, совместно именуемые Стороны заключили настоящее Дополнительное соглашение №_____ (далее – Соглашение) к Договору текущего банковского счета №_____от «___» _____ 20__г. (далее – Договор счета) о нижеследующем:

1. Термины, используемые в Соглашении

1.1. Система дистанционного банковского обслуживания (далее - ДБО) – система, предоставляющая Клиенту возможность управления своими банковскими счетами путём обмена документов в электронной форме (далее - электронные документы) между Клиентом и Банком через web-сайт Банка, доступ к которому осуществляется через сеть Интернет.

1.2. Регистрационное свидетельство – документ на бумажном носителе или электронный документ, выдаваемый Удостоверяющим центром для подтверждения соответствия электронной цифровой подписи требованиям, установленным Законом Республики Казахстан от 7 января 2003 года № 370-II «Об электронном документе и электронной цифровой подписи».

1.3. Электронная цифровая подпись (ЭЦП) – набор электронных цифровых символов, подтверждающих достоверность электронного

құжат.
1.3. Электрондық сандық қол (ЭСҚ) - электрондық құжаттың сенімділігін, оның тиесілігін және мазмұнының өзгермейтіндігін растайтын электрондық сандық белгілер жинағы (ЭСҚ). ЭСҚ электрондық құжат авторын және/немесе оны беру және құжатқа қол қойылған сәттен бастап өзгермегендігін растау іске асырылған түпнұсқаландыру құралын белгілейді.
1.4. Жабық кілт (құпия кілт) - Тіркеу куәлігінің иесіне белгілі және ЭСҚ құралын пайдаланумен ЭСҚ жасауға арналған электронды сандық белгілердің бірізділігі.
1.5. Ашық кілт (жария кілт) – электрондық сандық белгілердің бірізділігі және электрондық құжатта ЭСҚ түпнұсқалығын растауға арналған. Ашық кілт Тараптарға салдарынан Клиент зиян шегетін электрондық құжаттар құрастыруға, қол қоюға және Клиент шоттары бойынша пайда алмай қалатын қандай да бір операциялар жүргізуге мүмкіндік бермейді.
1.6. Кілттік тасымалдағыш - Клиент электрондық құжаттарға қол қою құқығы бар уәкілетті тұлғалардың жабық кілттерін сақтауға арналған Клиент пайдаланатын қорғалған электрондық құрылғы. Банк Клиентке Кілттік тасымалдағышты Қабылдау-беру актісі бойынша береді.
1.7. Куәландырушы орталық - ЭСҚ ашық кілтінің ЭСҚ жабық кілтіне сәйкестігін куәландыратын, қызметтің тиісті түріне аккредитациясы бар, сондай-ақ Тіркеу куәлігінің сенімділігін растайтын заңды тұлға.
1.8. Клиенттің бағдарламалық-техникалық құралы – Клиентке Жүйеде үшінші тұлғаларға өз есебінен Жүйеде жұмыс істеуі үшін қажетті компьютерлік жабдық және бағдарламалық құрал:
1) мынадай конфигурациядағы IBM PC үйлесімді дербес компьютер (бұдан әрі – «ДК»): процессор – Celeron 300, ОЗУ – 64 Мб бастап, 250 Мб кем емес бос көлемі бар қатты диск;
2) Windows Vista, Windows операциялық жүйесі;
3) Қосылған желілік немесе жергілікті принтер;
4) Компьютерде операциялық жүйеге орнатылған драйвері бар (Интернеттің ерекшеленген желісі жоқ болған жағдайда);
5) Телефон байланысының желісі және Интернеттің ерекшеленген желісі Ерекшеленген желі болған жағдайда ҚБҚ-да жұмыс істеу үшін прокси – серверде 443 ашық порт.
1.9. Электрондық құжат - қағаздық тасымалдағыштағы құжатқа тең мәнді құжат, онда ақпарат электрондық-сандық нысанда берілген және ЭСҚ арқылы куәландырылған.
1.10. КО ДСН-конверті - Тіркеу куәлігін алу кезінде Клиенттің пайдаланушысының жеке басын растау үшін пайдаланылатын Логиннен және Клиенттің ДСН-кодынан тұратын қорғалған құжат. ДСН-код жабық конвертке салынады. ДСН-кодты басып шығаруды КО жүргізеді, Клиентке беруді Банк жүргізеді.
1.11. Кіруді авторландыру және төлемдерді растау ОТР - электрондық құжаттарды алмастыру

документа, его принадлежность и неизменность содержания. ЭЦП устанавливает автора электронного документа и/или средство аутентификации, с использованием которого осуществлена его передача и подтверждение, что документ не был изменен с момента его подписания.
1.4. Закрытый ключ (секретный ключ) – последовательность электронных цифровых символов, известная владельцу Регистрационного свидетельства и предназначенная для создания ЭЦП с использованием средств ЭЦП
1.5. Открытый ключ (публичный ключ) – последовательность электронных цифровых символов и предназначенная для подтверждения подлинности ЭЦП в электронном документе. Открытый ключ не позволяет Сторонам формировать, подписывать электронные документы либо производить какие-либо операции по счетам Клиента, вследствие которых Клиент может понести ущерб, упущенную выгоду.
1.6. Ключевой носитель – защищенное электронное устройство, используемое Клиентом для хранения закрытых ключей уполномоченных лиц, имеющих право подписи электронных документов. Передается Банком Клиенту по Акту приема-передачи Ключевого носителя.
1.7. Удостоверяющий центр - юридическое лицо, имеющее аккредитацию на соответствующий вид деятельности, удостоверяющее соответствие открытого ключа ЭЦП закрытому ключу ЭЦП, а также подтверждающее достоверность Регистрационного свидетельства.
1.8. Программно-технические средства Клиента – компьютерное оборудование и программные средства необходимое Клиенту для работы в ДБО за свой счёт у третьих лиц:
1) IBM PC совместимый персональный компьютер (далее – «ПК») следующей конфигурации: процессор – от Celeron 300, ОЗУ – от 64 Мб, жесткий диск со свободным объемом не менее 250 Мб;
2) Операционная система Windows Vista, Windows
3) Подключенный сетевой или локальный принтер;
4) Модем с драйверами под установленную на компьютере операционную систему (в случае отсутствия выделенной линии Интернет);
5) Линия телефонной связи или выделенная линия Интернет. В случае выделенной линии открытый порт 443 на прокси – сервере для работы в ДБО.
1.9. Электронный документ - Документ, равнозначный документу на бумажном носителе, в котором информация представлена в электронно-цифровой форме и удостоверена посредством ЭЦП.
1.10. ПИН-конверт УЦ - защищенный документ, содержащий Логин и ПИН-код Клиента, используемый для подтверждения личности пользователя Клиента при получении Регистрационного свидетельства. ПИН-код печатается внутри закрытого конверта. Печать

операцияларын растау және ҚБҚ-ға авторландыру түрінде біржолғы сеанстық кілт көмегімен, оларды іздестіру e-Token PASS time based (e-Token PASS event based) құрылғысының көмегімен іске асырылады.
1.12. e-Token PASS time based - біржолғы парольдерді уақыты бойынша синхрондайтын құрылғы, олар белгіленген уақытта үнемі өзгереді.
1.13, e-Token PASS event based - біржолғы парольдерді оқиға бойынша синхрондайтын құрылғы.

2. Қосымша мәні
2.1. Банк:
2.1.1. Клиентке ҚБҚ-да осы Келісім мен Шот шартында қарастырылған талаптармен қызмет көрсетеді.
2.1.2. ҚБҚ-да операциялар жүргізу кезінде қауіпсіздікті күшейту мақсатында Негізгі тасымалдағыштарды және (немесе) e-Token PASS time based (e-Token PASS event based) пайдалануды ұсынады.
2.2. Клиент:
2.2.1. ҚБҚ-да жұмыс жүргізу кезінде e-Token PASS time based (e-Token PASS event based) құрылғысының көмегімен кіруді OTP авторландыру және төлемдерді растау.
2.2.2. ҚБҚ-да жұмыс істеу кезінде кірудің OTP авторландыруын пайдалану және e-Token PASS time based құрылғысының немесе ЭСҚ көмегімен төлемдерді растау.
2.2.3. Банктің Клиентті ҚБҚ-ға қосу және қызмет көрсету бойынша көрсететін барлық қызметтерінің ақысын Банктің операция жүргізу кезінде әрекет етуші Тарифтеріне (бұдан әрі - Банк Тарифтері) сәйкес осы Келісіммен қарастырылған талаптармен төлейді.
2.2.4. Уәкілетті тұлғаның ЭСҚ сақтау үшін Кілт тасымалдағыш немесе төлем құжаттарына қол қою құқығы бар e-Token PASS time based пайдаланады;
2.2.5. e-Token PASS time based (e-Token PASS event based) және (немесе) Тіркеу куәлігін, сондай-ақ КО-тан ЭСҚ кілттерді алады және оларды Банк берген Кілттік тасымалдағышта сақтайды (КО Банк Тіркеу куәліктерін шығаруға шарт жасасқан тұлға ғана бола алады).

3. Қызмет көрсету талаптары
3.1. Тараптар келесілерді мойындайды:
3.1.1. осы Келісім бойынша олар пайдаланатын телекоммуникациялар, ақпаратты өңдеу және сақтау жүйелері электронды құжаттарды қабылдау, беру, өңдеу және сақтау кезінде сенімді және тиімді жұмысты қамтамасыз ету үшін жеткілікті.
3.1.2. осы Келісім бойынша олар пайдаланатын қорғау жүйесі ақпараттарды санкцияланбаған қол жеткізуден қорғау, сондай-ақ авторлықты және электронды құжаттардың түпнұсқалығын растау үшін жеткілікті.
3.1.3. ҚБҚ-да операция жүргізу кезінде электронды нысанда пайдаланылатын ЭСҚ немесе e-Token

ПИН-конвертов производится УЦ, выдача Клиентам производится Банком.
1.11. OTP авторизация входа и подтверждение платежей - подтверждение операций по обмену электронными документами и авторизационный вход в ДБО, с помощью одноразовых сеансовых ключей, генерация которых осуществляется с помощью устройства e-Token PASS time based (e-Token PASS event based).
1.12. e-Token PASS time based - устройство, синхронизирующее по времени одноразовые пароли по времени, которые постоянно меняются в установленное время
1.13. e-Token PASS event based - устройство, синхронизирующее по времени одноразовые пароли по событию.

2. Предмет Соглашения
2.1. Банк:
2.1.1. Производит обслуживание Клиента в ДБО на условиях, предусмотренных настоящим Соглашением и Договором счета.
2.1.2. В целях усиления безопасности при проведении операций в ДБО предоставляет использовать Ключевые носители и (или) e-Token PASS time based (e-Token PASS event based).
2.2. Клиент:
2.2.1. При работе в ДБО использовать OTP авторизацию входа и подтверждение платежей, с помощью устройства e-Token PASS time based (e-Token PASS event based) и ЭЦП.
2.2.2. При работе в ДБО использовать OTP авторизацию входа и подтверждение платежей, с помощью устройства e-Token PASS time based или ЭЦП.
2.2.3. Оплачивает все услуги, оказываемые Банком по подключению и обслуживанию Клиента в ДБО в соответствии с Тарифами Банка, действующими на момент совершения операции (далее – Тарифы Банка) на условиях, предусмотренных настоящим Соглашением.
2.2.4. Использует Ключевой носитель для хранения ЭЦП уполномоченных лиц или e-Token PASS time based, имеющих право подписи платежных документов;
2.2.5. Получает e-Token PASS time based (e-Token PASS event based) и (или) Регистрационное свидетельство, а также ключи ЭЦП от УЦ, и хранит их на Ключевом носителе предоставленным Банком (УЦ может быть, только тот, с которым Банк заключил договор на выпуск Регистрационных свидетельств).

3. Условия оказания услуг
3.1. Стороны признают, что:
3.1.1. Используемые ими по настоящему Соглашению системы телекоммуникации, обработки и хранения информации достаточны для обеспечения надежной и эффективной работы при приеме, передаче, обработке и хранении электронных документов.

PASS time based куәландырылған "электронды құжаттар" заңды түрде қағаздық тасымалдағыштардағы құжаттарға теңдей мәнде және Тараптардың осы Келісім бойынша ұқсас құқықтар мен міндеттерді туындатады.

3.1.4. Клиенттің электронды құжаттарын Клиенттің уәкілетті тұлғалары ретінде өзінің ЭСҚ немесе e-Token PASS time based қол қоюға құқылы уәкілетті тұлғалар Клиенттің Банкке берген қойылған қол және мөр бедерінің үлгілеріне қарай қарай анықталады.

3.1.5. Электронды құжаттарға қол қоя алатын уәкілетті тұлғалар тізімі өзгерген жағдайда Клиент Банкке мұндай тұлғалардың өкілеттігін тоқтату туралы жазбаша өтінішті дереу жіберуге тиіс.

4. Электронды құжаттарды есеп айрысуларда қолдану тәртібі.

4.1. Клиенттен құжаттарды электронды түрде қабылдауды Банк тәулігіне 24 сағат, жылына 365 күнде жүргізеді.

4.2. Банкке ағымдағы Операциялық күнде валюталандыру күнімен, Астана уақыты бойынша сағат 17:00 дейінгі кезеңді қоса жіберілген құжаттарды Банк орындауға валюталандырудың ағымдағы күнімен қабылдайды. Банкке ағымдағы Операциялық күнде валюталандыру күнімен, Астана уақыты бойынша сағат 17:00 кейін жіберілген құжаттарды Банк орындауға келесі жұмыс күні қабылдайды, бұл ретте төлем тапсырмасын жазып беру күні Банктің құжатты орындаған күнгі ағымдағы күн болып есептеледі.

4.3. Электрондық құжаттар Қазақстан Республикасының Ұлттық Банкінің (бұдан әрі - ҚРҰБ) нормативтік құқықтық актілеріне сәйкес төлем құжаттарын ресімдеу ережелері және Қазақстан Республикасының басқа заңнамалық актілері, сондай-ақ Банктің ішкі нормативтік құжаттары бойынша ресімделуі тиіс және электрондық құжаттардың қағаздық тасымалдағыштардағы түпұсқаларына сәйкестігі талап етіледі.

4.4. Тараптардың әрқайсысы электронды нысанда екінші Тарапқа мынадай құжаттардың кез келгенін бере немесе ала алады:

- төлем тапсырмасы (оның ішінде жалақылық, зейнетақылық, кедендік және әлеуметтік төлемдер);
- шетел валютасын аударуға өтініш;
- валюта сатып алуға, сатуға өтініш;
- Клиент шоттары бойынша көшірмелер;
- Клиенттің банктік шоттарына ақшаның түскені туралы төлем құжаттарының электронды көшірмелері;
- Қазақстан Республикасы Ұлттық Банкінің нормативтік құқықтық актілерімен және Банктің ішкі нормативтік құжаттарымен белгіленген басқа төлем құжаттары.

Төлемдік емес сипаттағы басқа ақпаратты беруге

3.1.2. Используемые ими по настоящему Соглашению системы защиты информации, достаточны для защиты от несанкционированного доступа, а также подтверждения авторства и подлинности электронных документов.

3.1.3. Используемые при совершении операций в ДБО документы в электронной форме «электронные документы», заверенные ЭЦП или e-Token PASS time based, юридически равнозначны документам на бумажном носителе и порождают аналогичные им права и обязанности Сторон по настоящему Соглашению.

3.1.4. Уполномоченные лица, которые будут вправе подписывать своей ЭЦП или e-Token PASS time based электронные документы Клиента в качестве уполномоченных лиц Клиента, будут определяться исходя из представленных Клиентом в Банк документов с образцами подписей и оттиска печати.

3.1.5. В случае изменения списка уполномоченных лиц, которые могут подписывать электронные документы, Клиент должен незамедлительно направить в Банк письменное заявление о прекращении полномочий таких лиц.

4. Порядок применения электронных документов в расчетах

4.1. Прием документов в электронном виде от Клиента производится Банком 24 часа в сутки, 365 дней в году.

4.2. Документы, отправленные в Банк, датой валютирования текущего Операционного дня, включая период до 17:00 времени Астаны, принимаются Банком к исполнению текущей датой валютирования. Документы, отправленные в Банк датой валютирования текущего Операционного дня после 17:00 времени Астаны, принимаются Банком к исполнению на следующий рабочий день, при этом датой выписки платежного поручения будет считаться текущая дата в день исполнения документа Банком.

4.3. Электронные документы должны быть оформлены в соответствии с нормативными правовыми актами Национального Банка Республики Казахстан (далее – НБРК) по правилам оформления платежных документов и иными законодательными актами Республики Казахстан, а также внутренними нормативными документами Банка и предполагают соответствие реквизитов электронных документов оригиналам на бумажных носителях.

4.4. Каждая из Сторон может в электронной форме передавать другой Стороне или получать от другой Стороны любой из следующих документов:

- платежное поручение (в том числе зарплатные, пенсионные, таможенные и социальные платежи);
- заявление на перевод иностранной валюты;
- заявление на покупку, продажу валюты;
- выписки по счетам Клиента;
- электронные копии платежных документов о поступлении денег на банковские счета Клиента;

рұқсат етіледі, бірақ бұл ақпарат осы қосымша бойынша міндеттемелердің пайда болу негіздемесі болып табылады.

4.5. Электронды құжат тиісті түрде ресімделген, ЭСҚ немесе e-Token PASS time based куәландырылған, ҚБҚ пайдаланумен беруші Тарап жеткізген, ал қабылдаушы Тарап тексерген және қабылдаған Клиент пен Банктің осы Келісім бойынша міндеттемелерін туындатады.

5. Тараптардың құқықтары мен міндеттері

5.1. Тараптардың міндеттері:

5.1.1. Электрондық құжаттарды пайдалану кезінде ҚРҰБ ережелерін және талаптарын, Қазақстан Республикасының заңнамасын, осы Келісімді, сондай-ақ Банктің ішкі нормативтік құжаттарын басшылыққа алу;

5.1.2. Телекоммуникация, ақпаратты өңдеу, сақтау және қорғау жүйесін тек жұмыс істейтін және жарамды, ҚБҚ мен Тараптарға зиян келтіретін компьютерлік вирус пен бағдарламалардың жоқтығы тексерілген жабдықта пайдалану;

5.1.3. Үшінші тарапқа (Қазақстан Республикасының қолданыстағы заңнамасында қарастырылған жағдайларды қоспағанда) ҚБҚ қолданылатын ақпаратты қорғаудың нақты тәсілдерін жария етпеу;

5.1.4. Екінші Тарапқа телефон шалу және кейіннен Банкке жазбаша хабарлама жіберу арқылы ҚБҚ-ға және құпия кілттерге санкцияланбаған қол жеткізу туралы күдік, сондай-ақ телекоммуникация, ақпаратты өңдеу, сақтау және қорғау жүйелерінің бағдарламалық-техникалық құралдарының жоғалу, ұрлану немесе бүліну жағдайлары туралы жоғарыда көрсетілген бағдарламалық-техникалық құралдарды жұмыс істейтін қалыпта ұстау үшін кілттерді ауыстыру және басқа екінші Тараппен келісілген әрекеттерді жасау үшін дереу хабарлау;

5.1.5. Өзінің жабық кілті (құпия кілт) немесе Token PASS time based жария болған жағдайда бұл кілтті пайдалануды дереу тоқтату және екінші Тарапты оқшаулау үшін жария болғаны туралы хабардар ету немесе екінші Тараптан ҚБҚ-ға санкцияланбаған қол жеткізуге күдіктену туралы хабарлама алған жағдайда екінші Тараптың электронды құжаттармен жасалған барлық операцияларын дереу оқшаулау;

5.1.6. Электрондық құжаттардағы ақпараттың құпиялылығын қамтамасыз ету;

5.1.7. Екінші Тараптың талап етуі бойынша келесі жұмыс күнінен кешіктірмей ҚБҚ арқылы жіберілген/алынған тиісті түрде ресімделген электрондық құжаттардың қағаздағы даналарын беру.

5.1.8. Тараптар өзара келісім кезінде телекоммуникациялар, ақпаратты өңдеу, сақтау және қорғау жүйесін ауыстыруды жүргізуге құқығы бар.

- иные платежные документы, установленные нормативными правовыми актами Национального Банка Республики Казахстан и внутренними нормативными документами Банка.

Допускается передача другой информации неплатежного характера, но эта информация не является основанием возникновения обязательств по настоящему Соглашению.

4.5. Электронный документ порождает обязательства Клиента и Банка по настоящему Соглашению, если он надлежащим образом оформлен, заверен ЭЦП или e-Token PASS time based, доставлен с использованием ДБО передающей Стороной, а принимающей Стороной проверен и принят.

5. Права и обязанности Сторон

5.1. Стороны обязуются:

5.1.1. При использовании электронных документов руководствоваться правилами и требованиями НБРК, законодательством Республики Казахстан, настоящим Соглашению, а также внутренними нормативными документами Банка;

5.1.2. Использовать ДБО телекоммуникаций, обработки, хранения и защиты информации только на работоспособном и исправном оборудовании, проверенном на отсутствие компьютерных вирусов и программ, способных нанести вред ДБО и Сторонам;

5.1.3. Не разглашать третьей стороне (за исключением случаев, предусмотренных действующим законодательством Республики Казахстан, конкретные способы защиты информации, применяемые в ДБО;

5.1.4. Немедленно информировать другую Сторону посредством телефонного звонка и в последующем отправки письменного уведомления Банку обо всех случаях подозрений на несанкционированный доступ к ДБО и к секретным ключам, а также утраты, похищения или повреждения программно-технических средств ДБО телекоммуникации, обработки, хранения и защиты информации для проведения смены ключей и других согласованных действий с другой Стороной по поддержанию в рабочем состоянии вышеуказанных программно-технических средств;

5.1.5. В случае компрометации своего закрытого ключа (секретный ключ) или Token PASS time based немедленно прекратить пользоваться этим ключом и уведомить другую Сторону о факте компрометации для блокирования, или в случае получения уведомления от другой Стороны о подозрении на несанкционированный доступ к ДБО немедленно блокировать все операции с электронными документами другой Стороны;

5.1.6. Обеспечивать конфиденциальность информации, содержащейся в электронных документах;

5.1.7. По требованию другой Стороны предоставить не позднее следующего рабочего дня соответствующим образом оформленные

5.2. Банктің міндеттері:

5.2.1. Осы Келісімді жасағаннан және Клиент комиссияны Тарифтерге сәйкес тиісті түрде төленгеннен кейін Клиенттің ҚБҚ-ға қолжетімділігін тіркеу, оған ҚБҚ-мен жұмыс бойынша пайдаланушы нұсқаулығынан тұратын нұсқамалық/оқыту материалдарын беру және Клиентке ҚБҚ-да тиісті түрде банктік қызмет көрсетуді қамтамасыз ету.

5.2.2. ҚБҚ-ны, куәландырылған ЭСҚ және КО немесе Клиенттің e-Token PASS time based растаған пайдаланумен Банкке берілген ақшаны Клиент шотынан аудару туралы өкімді орындау;

5.2.3. Клиентке оның банктік шоттары бойынша жүргізілген операциялар бойынша ақпарат беру.

5.3. Банктің құқықтары:

5.3.1. Мынадай жағдайда электронды құжатты орындаудан бас тарту:

- электрондық құжаттарға жарамсыз/оқшауланған ЭСҚ кілтімен және (немесе) e-Token PASS time based қол қою;
- егер ЭСҚ және (немесе) e-Token PASS time based тиісті электрондық құжатқа қол қоюға өкілеттігі жоқ тұлғаға тиесілі болса;
- электрондық құжаттарға Банкке берілген қол қою үлгісі мен Клиент мөрі жоқ құжаттар жоқ тұлға қол қойғанда (бұл Қазақстан Республикасының заңнамасына сәйкес талап етілген жағдайда);
- егер электрондық құжат осы Келісімнің талаптарын және Қазақстан Республикасы заңнамасының талаптарын бұзумен жасалған және берілген болса;
- Қазақстан Республикасы заңнамасында, сондай-ақ Банктің ішкі нормативтік құжаттарында қарастырылған басқа жағдайларда;

5.3.2. Клиентке ҚБҚ бойынша хабарлама жіберу арқылы Клиентті алдын ала хабарландыра отырып, ҚБҚ қорғау тетігіне өзгерістер енгізу;

5.3.3. Клиентті мынадай жағдайда ҚБҚ-дан ажырату:

- Клиенттің Тіркеу куәлігінің әрекет ету мерзімі аяқталғанда;
- шот бойынша қозғалыстың немесе Клиент шотында 6 (алты) ай бойы ақшаның жоқ болуы;
- ҚБҚ-ға қызмет көрсетілгені үшін 6 (алты) ай бойы комиссия төлемеу;
- ҚБҚ-ға үшінші тұлғалар санкцияламай қол жеткізу туралы күдік туындағанда;
- ҚБҚ-ны 6 (алты) ай бойы пайдаланбау.

5.3.4. Клиенттің Тіркеу куәлігі берілмегенде Банк Клиенттің жұмыстан шыққан/ ауыстырылған өкіліне қолжетімділікті оқшаулайды;

5.3.5. Клиенттің қолданыстағы Тіркеу

бумажные экземпляры электронных документов, направленных/полученных через ДБО.

5.1.8. Стороны имеют право при взаимном согласии производить замену систем телекоммуникаций, обработки, хранения и защиты информации.

5.2.Банк обязан:

5.2.1. После заключения настоящего Соглашения и надлежащей оплаты Клиентом комиссии за подключение к ДБО в соответствии с Тарифами Банка, провести регистрацию доступа Клиента к ДБО предоставить ему инструктивные/обучающие материалы, содержащие руководство пользователя по работе с ДБО и обеспечить надлежащее банковское обслуживание Клиента в ДБО.

5.2.2. Выполнять распоряжения на перевод денег со счета Клиента, переданные в Банк с использованием ДБО, заверенные ЭЦП и подтвержденные УЦ или e-Token PASS time based Клиента.;

5.2.3. Предоставлять Клиенту информацию по операциям, проведенным по его банковским счетам.

5.3. Банк вправе:

5.3.1. Отказать в исполнении электронного документа Клиента в случае:

- подписания электронных документов недействительным/заблокированным ключом ЭЦП и (или) e-Token PASS time based;
- если ЭЦП и (или) e-Token PASS time based принадлежит лицу, не имеющему полномочий на подписание соответствующего электронного документа;
- подписания электронных документов лицом отсутствующим в представленном в Банк документе с образцом подписи и печати Клиента (в случае, когда это требуется в соответствии с законодательством Республики Казахстан);
- если электронный документ составлен и представлен с нарушением условий настоящего Соглашения и требований законодательства Республики Казахстан;
- в иных случаях, предусмотренных законодательством Республики Казахстан, а также внутренними нормативными документами Банка;

5.3.2. Вносить изменения в механизмы защиты ДБО, с предварительным уведомлением Клиента путем направления уведомления Клиенту по ДБО;

5.3.3.Отключить Клиента от ДБО в случае:

- истечения срока действия Регистрационного свидетельства Клиента;
- отсутствия движения по счету либо отсутствия денег на счете Клиента в течение 6 (шести) месяцев подряд;
- неуплаты комиссии за обслуживание ДБО в течение 6 (шести) месяцев подряд;
- возникновения подозрения о несанкционированном доступе к ДБО третьих лиц
- не использование ДБО в течении 6 (шести) месяцев подряд.

куәлігі болмаған жағдайда ҚБҚ қызметін көрсетпеу.
5.3.6. ҚБҚ-да жұмыс істеу үшін пайдаланылатын банктік шот жабылғанда Клиенттің бастамасы бойынша немесе Қазақстан Республикасының қолданыстағы Заңнамасына сәйкес Банктің біржақты тәртіппен алдын ала хабарландырусыз Клиенттің ҚБҚ-ға қолжетімділігін алып тастауға құқығы бар;
5.3.7. Осы Келісім бұзылған кезде ҚБҚ-да Клиенттің Тіркеу куәлігін оқшаулау;
5.3.8. Мынадай жағдайда Клиентті ҚБҚ-дан уақытша оқшаулау:
- ҚБҚ-да қашықтан банктік қызмет көрсетуді орнату актісін бермеген;
- ҚБҚ-ға қосылған сәттен бастап 14 (он төрт) күн ішінде ҚБҚ пайдаланбау.
5.3.9. Шоттан акцептсіз тәртіпте тікелей дебеттеу арқылы ай сайын Банктің қолданыстағы тарифтеріне сәйкес Банктің ҚБҚ қызмет көрсеткені үшін абоненттік төлемді есептен шығару. Шотта қажетті ақша сомасы болмаған жағдайда Банкте ашылған кез келген басқа шоттан алу.
5.3.10. ҚБҚ қызмет көрсетілгені үшін абоненттік төлем ҚБҚ бойынша операциялардың болғанына байланыссыз есептеледі және өтеледі, ал Шотта (-тарда) өтеу үшін қажетті ақша сомасы болмаған кезде Шотта бар ақша сомасы шегінде өтеледі. Клиенттің шотына ақша түскен кезде төленбеген айлар үшін комиссиялық сыйақы ұсталады.

5.4. Клиенттің міндеттері:
5.4.1. осы Келісімге қол қойылғаннан кейін 3 (үш) жұмыс күні ішінде қолма-қол ақшасыз немесе қолма-қол ақшамен Клиентті ҚБҚ-ға қосу үшін Банк Тарифтеріне сәйкес ақы төлеу;
5.4.2. ҚБҚ, e-Token PASS time based (e-Token PASS event based) пайдаланумен байланысты барлық ақпаратты,, оның ішінде ҚБҚ-да жұмыс істеуге арналған барлық құпия сөздер мен кодтарды, Кілттік тасымалдағыштағы ашық (жария кілт) және жабық кілт (құпия кілт), сондай-ақ осы Қосымша келісімді орындаумен байланысты басқа ақпараттың құпиялылығын сақтау.
5.4.3. Жабық кілт (құпия кілт) бар Кілттік тасымалдағышты және e-Token PASS time based (e-Token PASS event based) уәкілетті емес тұлғалардың қолы жетпейтін сенімді жерде сақтау;
5.4.4. Тіркеу нөмірін пайдалану кезінде ашық кілтті (жария кілт) және жабық кілтті (құпия кілт) Кілттік тасымалдағышта сақтауды дербес жүргізу;
5.4.5. Кілттік тасымалдағышты нұсқамалық/оқыту материалына сәйкес тіркеу куәлігін пайдалану кезінде ҚБҚ-ғы жұмыс аяқталғаннан кейін дұрыс ажырату;
5.4.6. ҚБҚ орнатылған компьютерге уәкілетті емес тұлғалардың қол жеткізуін болдырмау мақсатында қауіпсіздіктің барлық ұйымдастыру шараларын қабылдау;

5.3.4.При непредставлении Регистрационного свидетельства Клиентом, Банк блокирует доступ в ДБО уволившегося/замененного представителя Клиента;
5.3.5Не предоставлять услуги ДБО в случае отсутствия у Клиента действительного Регистрационного свидетельства.
5.3.6.При закрытии банковского счета, используемого для работы в ДБО, по инициативе Клиента, либо в соответствии с действующим Законодательством Республики Казахстан), Банк имеет право в одностороннем порядке без предварительного уведомления отключить Клиенту доступ в ДБО;
5.3.7.При расторжении настоящего Соглашения блокировать в ДБО Регистрационное свидетельство Клиента;
5.3.8.Временно блокировать Клиента от ДБО в случае:
- не предоставления акта установки в ДБО дистанционного банковского обслуживания;
- не использования ДБО в течении 14 (четырнадцати) дней с момента подключения к ДБО.
5.3.9. Ежемесячно, путем прямого дебетования в безакцептном порядке списывать со Счета (-ов) абонентскую плату за обслуживание ДБО Банка, согласно действующим тарифам Банка. В случае отсутствия необходимой суммы денег на Счете, с любого другого счета, открытого в Банке.
5.3.10. Абонентская плата за обслуживание в ДБО начисляется и погашается независимо от наличия операций по ДБО, а при отсутствии на Счете _(-ах) необходимой для погашения суммы денег, погашается в пределах имеющейся суммы денег. При поступления денег на счета Клиента, комиссионное вознаграждение удерживается по факту за неоплаченные месяцы.
5.4.Клиент обязан:
5.4.1. Произвести оплату за подключение Клиента к ДБО согласно Тарифам Банка в течение 3 (трёх) рабочих дней после подписания настоящего Соглашения в безналичном или наличном порядке;
5.4.2. Сохранять конфиденциальность всей информации, связанной с использованием ДБО, e-Token PASS time based (e-Token PASS event based) в том числе все пароли и коды, предназначенные для работы в ДБО, открытый (публичный ключ) и закрытый ключ (секретный ключ) на Ключевом носителе, а также иную информацию, связанную с исполнением настоящего Дополнительного соглашения.
5.4.3. Хранить Ключевой носитель с закрытым ключом (секретным ключом) и e-Token PASS time based (e-Token PASS event based) в надежном месте, исключающем доступ к ней неуполномоченных лиц;
5.4.4. Самостоятельно производить сохранение открытого (публичного ключа) и закрытого ключа (секретного ключа) на Ключевой носитель, при спользовании регистрационного свидетельства;
5.4.5. Корректно отключать Ключевой носитель в

ҚБҚ талап етуі бойынша құпия сөзді соңғы ауыстырған сәттен бастап 30 (60) күнтізбелік күн аяқталғанда құпия сөзді ауыстыру операциясын жүргізу;

5.4.7. Жабық (құпия) кілтті және e-Token PASS time based (e-Token PASS event based) сақтау кезінде қауіпсіздікті күшейту мақсатында, және ҚБҚ-да операция жүргізу кезінде Клиент 2.2.3-т. көрсетілген қауіпсіздік шараларын пайдаланады, қызметтен бас тартқан жағдайда клиент жазбаша бас тартады және қауіпсіздіктің қосымша шараларынан бас тарту нәтижесінде шеккен зиян үшін толық жауапкершілікте болады.

5.4.8. Банк осы Келісім бойынша белгілеген бағдарламалық-техникалық жасақтаманы жаңартпау, бөлшектемеу, тираждамау немесе үшінші тұлғаға бермеу;

5.4.9. Тіркеу куәлігін пайдалану кезінде еркін қолжетімділіктегі жария шарт жасау. Жария шарттың үлгісін ашық көздерден алуға болады (Банк, КО web-сайт УЦ, тікелей КО-да) КО өзара есеп айырысуды Клиент Банктің қатысуынсыз дербес жүргізеді;

5.4.10. Тіркеу куәлігін пайдалану кезінде (кемінде жылына 1 рет) және Тіркеу куәлігінің әрекет ету мерзімі аяқталғанға дейін 7 (жеті) жұмыс күнінен кешіктірмей өз есебінен КО жаңа Тіркеу куәлігін алу және кілттерді ауыстыру - жабық кілтті (құпия кілтті) және тиісті ашық кілтті (жария кілтті) түрлендіру;

5.4.11. Жаңасын (ларын) алғаннан кейін Банкке қолданыстағы Тіркеу куәлігін (терін) беру.

5.4.12. ҚБҚ жұмысы үшін зиянды бағдарламалардан сақталған, бөлінген бағдарламалық-техникалық құралды жұмыс үшін беру және әлеуметтік желілерге қосу;

5.4.13. Осы Келісімге сәйкес пайдаланылатын өзінің бағдарламалық-техникалық құралдарын жұмыс істейтін күйде ұстау;

5.4.14. Уақытында, аптасына кемінде 1 рет бағдарламалық-техникалық құралдарда (компьютерде) вирустың бар екендігін тексеру және вирусқа қарсы бағдарламаларды жаңартуды белгілеу.

5.4.15. Банкке электронды құжаттарды, куәландырылған Клиенттің ЭСҚ немесе e-Token PASS time based беру;

5.4.16. Дереу 3 (үш) жұмыс күні ішінде жазбаша немесе ҚБҚ арқылы Банк Клиент Шоты бойынша жүргізетін опрерацияларға әсер етуі мүмкін барлық өзгерістер (телефон нөмірлері, электронды почта мекенжайлары), оның ішінде Клиент атауының, оның орналасқан жерінің, Шотқа ие болуы құқығына ие тұлғалардың өзгертілгені, уәкілетті тұлғалардың өзгертілгені туралы мұндай өзгерістерді растайтын құжаттардың түпнұсқаларын бере отырып, Банкке хабарлау. Өйтпеген жағдайда Банк онда Шот бойынша операциялар жүргізуге әсер ететін болған оқиғалар туралы ақпарат жоқ болғанда жасалған әрекет (әрекетсіздік) үшін жауапкершілікте болмайды;

5.4.17. Жабық кілт (құпия кілт), e-Token PASS time

соответствии с инструктивным/обучающим материалом каждый раз после завершения работы в ДБО, при спользовании регистрационного свидетельства;

5.4.6. Принять все организационные меры безопасности для предотвращения несанкционированного доступа неуполномоченных лиц к компьютеру, на котором установлена ДБО;

Производить операцию смены пароля по требованию ДБО – по истечении 30 (60) календарных дней с момента последней смены пароля;

5.4.7. В целях усиления безопасности при хранении закрытого (секретного) ключа и e-Token PASS time based (e-Token PASS event based), а также при проведении операций в ДБО Клиент использует меры безопасности, указанные в п., 2.2.3, в случае отказа от услуг клиент письменно отказывается и несет полную ответственность за убытки, понесенные в результате отказа от дополнительных меры безопасности.

5.4.8. Не модифицировать, не декомпилировать, не тиражировать или передавать третьей стороне программно-техническое обеспечение, установленное Банком по настоящему Соглашению;

5.4.9. Заключить с УЦ публичный договор, находящийся в свободном доступе, при спользовании регистрационного свидетельства. Шаблон публичного приложения можно получить из открытых источников (Банк, web-сайт УЦ, непосредственно в УЦ). Взаиморасчеты с УЦ производятся Клиентом самостоятельно без участия Банка;

5.4.10. Периодически, при использовании регистрационного свидетельства, (не реже 1 раза в год) самостоятельно и за свой счет в срок не позднее 7 (семи) рабочих дней до истечения срока действия Регистрационного свидетельства получать от УЦ новое Регистрационное свидетельство и проводить замену ключей – генерировать закрытый ключ (секретный ключ) и соответствующий открытый ключ (публичный ключ);

5.4.11. После получения нового(-ых) предоставлять в Банк действительное(-ные) Регистрационное(-ые) свидетельство(-а).

5.4.12. Предоставить для работы ДБО выделенное программно-техническое средство, защищенное от вредоносных программ и подключения к социальным сетям;

5.4.13. Поддерживать в рабочем состоянии свои программно-технические средства, используемые в соответствии с настоящим Соглашением;

5.4.14. Своевременно, но не реже 1 раза в неделю проверять программно - технические средства (компьютер) на наличие вирусов и устанавливать обновление антивирусных программ.

5.4.15. Предоставлять в Банк электронные документы, заверенные ЭЦП или e-Token PASS time based Клиента;

5.4.16. Незамедлительно в течение 3 (трех)

based жоғалған немесе басқаша жария болған жағдайда және/немесе Клиентке тиесілі банктік шоттар бойынша санкцияланбаған операциялар жүргізілгеніне күдіктену кезінде Банкке есептік жазуды оқшаулау талабымен дереу өтініш жасау, бұл ретте Клиент қысқа мерзімде e-Token PASS time based немесе кілттерді және ЭСҚ Тіркеу куәлігін КО ауыстыруға және жаңа Тіркеу куәлігін Банкке беруге міндетті.

5.4.18. ҚБҚ бағдарламалық жасақтамасын тираждау, дизассемблирлеу жағдайында Клиент Банкке осыған байланысты шеккен кез келген шығынды, жанама шығынды қоса, толық көлемде өтеу.

5.4.19. Клиенттің осы Келісімнің және нұсқамалық материалдардың талаптарын сақтамауы нәтижесінде шеккен шығындарын Банкке өтеу;

5.4.20. ҚБҚ ажырату кезінде Банкке берілген құрылғыларды қайтару: e-Token PASS time based (e-Token PASS event based), кілттік тасымалдағыш;

5.4.21. Банкке ҚБҚ қызмет көрсетілгені үшін абоненттік төлемді осы Келісімде қарастырылған талаптарда төлеу. Банкте ашылған Клиенттің шоттарында қажетті ақша сомасы болмаған жағдайда Клиент комиссиялық сыйақыны Банктің тиісті талабы қойылған мезеттен бастап 3 (үш) жұмыс күні ішінде Банкке төлейді.

5.5. Клиенттің құқықтары:

5.5.1. ҚБҚ толық кешенді қызметін осы Келісімде қарастырылған талаптармен пайдалану;

5.5.2. Өзінің банктік шоттарындағы ақшаға өздігінше иелік ету;

5.5.3. Банкке КО Тіркеу куәлігін және (немесе) e-Token PASS time based (e-Token PASS event based) алу кезінде КО Клиенттің құжаттарын беру туралы сенімхат беру. Өйтпеген жағдайда Клиент Тіркеу куәлігін және (немесе) e-Token PASS time based (e-Token PASS event based) өздігінше алады және Банкке береді.

5.5.4. Жаңа Кілттік тасымалдағыш және (немесе) e-Token PASS time based (e-Token PASS event based) алу үшін (жоғалған, бүлінген және т.б. кезінде) Банкке өтініш жасау және Банк тарифтеріне сәйкес ақы төлеу.

6. Тараптардың жауапкершіліктері

6.1. Тараптардың бірі электрондық құжаттарды пайдалану нәтижесінде, сондай-ақ қате электрондық құжаттарды орындау кезінде, егер бұл құжаттарды Тараптардың бірі тиісті түрде орындаса, ал екінші Тарап тексерген және қабылдаған болса, шеккен шығыстар үшін Тараптар жауапкершілікте болмайды.

рабочих дней письменно либо посредством ДБО сообщать Банку обо всех изменениях (номеров телефонов, адреса электронной почты) которые могут повлиять на проводимые Банком операции по Счету Клиента, в том числе, об изменении наименования Клиента, его местонахождения, об изменении лиц, обладающих правом распоряжения Счетом, смене уполномоченных лиц с представлением оригиналов документов, подтверждающих такие изменения. В противном случае, Банк не несет ответственности за действия (бездействие), совершенные при отсутствии у него информации о произошедших изменениях, влияющих на проведение операций по Счету;

5.4.17. В случае утери или иной компрометации закрытого ключа (секретного ключа), e-Token PASS time based и/или при подозрении случаев проведения несанкционированных операций по банковским счетам, принадлежащим Клиенту, незамедлительно обратиться в Банк с требованием блокирования учетной записи, при этом Клиент обязан в кратчайшие сроки поменять e-Token PASS time based или ключи и Регистрационное свидетельство ЭЦП в УЦ и предоставить новое Регистрационное свидетельство в Банк.

5.4.18. В случае тиражирования, дизассемблирования программного обеспечения ДБО Клиентом возместить Банку в полном объеме любые понесенные в связи с этим убытки, включая, косвенные убытки.

5.4.19. Возместить Банку все убытки, понесенные последним в результате несоблюдения Клиентом условий настоящего Соглашения и инструктивных материалов;

5.4.20. При отключении от ДБО возвратить Банку выданные устройства: e-Token PASS time based (e-Token PASS event based), ключевой носитель.

5.4.21. Оплачивать абонентскую плату за обслуживание ДБО Банку на условиях, предусмотренных настоящим Соглашением. В случае отсутствия необходимой суммы денег на счетах Клиента, открытых в Банке, Клиент производит оплату комиссионного вознаграждения Банка в течение 3(трех) рабочих дней с момента предъявления соответствующего требования Банком.

5.5. Клиент вправе:

5.5.1. Пользоваться полным комплексом услуг ДБО на условиях, предусмотренных настоящим Соглашением;

5.5.2. Самостоятельно распоряжаться деньгами на своих банковских счетах;

5.5.3. Предоставить Банку доверенность на передачу документов Клиента в УЦ при получение Регистрационного свидетельства от УЦ и (или) e-Token PASS time based (e-Token PASS event based). В противном случае Клиент самостоятельно получает и предоставляет в Банк Регистрационное свидетельство и (или) e-Token PASS time based (e-

6.2. Сақ болмаудан, оның ішінде Клиенттің ұқыпсыздығынан немесе қасақана ниетінен мүмкін болса, кез келген негіздемеде бойынша ҚБҚ кіру үшін деректері немесе кілттері, e-Token PASS time based қолжетімді болғаны үшін Клиенттің контрагенттерін қоса, бірақ мұнымен шектелмей, үшінші тұлғаларды кез келген әрекеттерінің нәтижесінде Клиенттің шеккен шығыстары үшін Банк жауапкершілікте болмайды,.
6.3. Клиент Электронды құжаттардың және ондағы мәліметтердің дұрыс ресімделуі үшін жауапкершілікте болады.
6.4. Клиент e-Token PASS time based мен жабық кілт (құпия кілт) сақталатын Кілттік тасымалдағыштың сақталуы үшін жауап береді.
6.5. Клиентке Банк есептік жазбаны оқшаулау мезетіне дейін Клиент ҚБҚ-да e-Token PASS time based және (немесе) кілттік тасымалдағышты пайдаланумен жасалған банктік шоттар бойынша жүргізілген операциялар үшін жауапкершілікте болады.
6.6. Банк Клиент алдында Клиент тапсырмаларының дұрыстығы және уақытында орындалуы үшін жауапкершілікте болады. Бұл ретте Банктің жауапкершілігі егер Банктің ішкі нормативтік құжаттарында және Қазақстан Республикасының заңнамасында белгіленген санкцияланбаған төлемнен қорғаудың барлық құралдарын пайдаланбаған болса ғана басталады және Клиент мұнымен сөзсіз келіседі.
6.7. Банк e-Token PASS time based және Кілттік тасымалдағыштың, Клиент компьютерінің қатты дискісінде орналастырылған төлем құжаттары мен көшірмелері мұрағаттарының сақталуы үшін жауапкершілікте болмайды.
6.8. Банк ҚБҚ-ның қызмет етуіне айтарлықтай әсер ететін табиғи апаттар, электр қуатын өшіру, байланыс желісінің бүлінуі түріндегі еңсерілмес күштер әрекеттерінің салдарынан туындаған ҚБҚ-ның тоқтатылғаны үшін жауапкершілікте болмайды. Банк сондай-ақ шот бойынша операциялар Клиенттің қатесі нәтижесінде, басқа Банктердің, есеп айырысу орталықтарының (немесе банк аралық есеп айырысуды іске асыратын басқа органдардың) кінәсінен кешіктірілсе, жауапкершілікте болмайды.
6.9. Банк Клиенттің төлем құжаттарын дұрыс ресімдемегені салдарынан (қате деректемелер, қос жазбалар, төлем алушының дұрыс жазылмаған мекенжайы және т.б. және т.с.с.), сондай-ақ Клиент пайдасына ақы төлейтін тұлғалар кінәсінен болған қате, бас тарту немесе кешіктіру салдарынан болған зиян үшін жауапкершілікте болмайды;
6.10. Банк Клиенттің өзінің құпия сөзін жария еткені немесе мәліметтерді шифрлауға арналған негізгі ақпаратты үшінші тұлғаларға себебіне байланыссыз бергені салдарынан туындаған зиян үшін жауапкершілікте болмайды.
6.11. Сақ болмаудан, оның ішінде Клиенттің ұқыпсыздығынан немесе қасақана ниетінен мүмкін болса, оның ішінде Тараптар осы Қосымша келісімнің барлық қосымшаларын ескере отырып Token PASS event based).
5.5.4. Получить новый Ключевой носитель и (или) e-Token PASS time based (e-Token PASS event based) (при утере, повреждении и т.д.) обратиться в Банк и внести оплату согласно Тарифам Банка.

6. Ответственность Сторон

6.1. Стороны не несут ответственности за убытки, понесенные одной из Сторон в результате использования электронных документов, в том числе при исполнении ошибочных электронных документов, если эти документы ненадлежащим образом одной Стороной оформлены и доставлены, а другой Стороной проверены и приняты.
6.2. Банк не несет ответственности за убытки, понесенные Клиентом в результате любых действий третьих лиц, включая, но, не ограничиваясь, контрагентами Клиента, которым по любым основаниям стали доступны данные для входа в ДБО или ключи, e-Token PASS time based если это стало возможным по неосторожности, в том числе включая небрежность, или умысел Клиента.
6.3. Клиент несет ответственность за правильность оформления Электронных документов и сведений, содержащихся в них.
6.4. Клиент несет ответственность за сохранность e-Token PASS time based и Ключевого носителя, на котором храниться закрытый ключ (секретный Ключ).
6.5. Клиент несет ответственность за операции по банковским счетам, совершенные в ДБО с использованием e-Token PASS time based и (или) Ключевого носителя, до момента блокирования учетной записи Клиенту Банком.
6.6. Банк несет ответственность перед Клиентом за правильность и своевременность выполнения поручений Клиента. При этом ответственность Банка наступает, и Клиент с этим, безусловно, согласен, только в том случае, если Банк не использовал все средства защиты от несанкционированного платежа, установленные внутренними нормативными документами Банка и законодательством Республики Казахстан.
6.7. Банк не несет ответственности за сохранность e-Token PASS time based и Ключевого носителя, архивов платежных документов и выписок, размещенных на жестком диске компьютера Клиента.
6.8. Банк не несет ответственности за прекращение использования ДБО, возникшее вследствие действия непреодолимой силы, существенно влияющей на функционирование ДБО, в виде стихийных бедствий, отключения электроэнергии, повреждений линий связи. Банк также не несет ответственности по настоящему Соглашению, если операции по счету задерживаются в результате ошибок Клиента, по вине других Банков, расчетных центров (или других органов, осуществляющих межбанковские расчеты).

онымен белгіленген және келісімделген барлық қауіпсіздік шараларын қолданбау себебінен болса, кез келген негіздемеде бойынша Логин / Құпия сөз, e-Token PASS time based және (немесе) кілттер қолжетімді болғаны үшін Клиенттің контрагенттерін қоса, бірақ мұнымен шектелмей, үшінші тұлғаларды кез келген әрекеттерінің нәтижесінде Клиенттің шеккен шығыстары үшін Банк жауапкершілікте болмайды.

7. Ерекше талаптар

7.1. Осы Келісімнің Тараптары Клиенттің Келісім Тараптары келіскен санкцияланбаған төлемдерден (ҚБҚ-ға қол жеткізуден) қорғаудың барлық құралдарын пайдалануға, ал Банк Банктің ішкі нормативтік құжаттарында және Қазақстан Республикасының заңнамасында белгіленген қорғау құралдарын пайдалану міндетті екендігін сөзсіз растайды және қайтарып алынбайтын келісімдерін береді. Бұл ретте Клиент Банктің міндеттері Қорғау құралдары туралы келісім ережелерін сақтаумен шектелетінін; және Клиент атынан сақтықсыз, Клиенттің кінәсінен немесе кінәсінсіз немесе үшінші тұлғалардың (оның ішінде Клиент қызметкерлерінің) кінәсінен жіберілген Клиент шоттарына қолжетімділік орын алып, нәтижесінде төлем жүргізілген болса (ҚБҚ-ға қолжетімділік) Клиент тарапынан санкцияланған деп сөзсіз есептелетінін түсінеді. Банк өз тарапынан Банкке Клиент атынан/тарапынан түскен электрондық құжаттың (төлем құжатының) әрқайсысын және кез келгенін алу кезінде талаптарды сақтауға және көрсетілген құралдарды қолдануға міндеттенеді.

7.2.Клиент міндетті түрде Кілттік тасымалдағышты немесе e-Token PASS time based пайдаланады.

- Кілттік тасымалдағыш және o e-Token PASS time based құрылғыларын Банк тікелей Клиентке/Клиенттің уәкілетті өкіліне береді. Кілттік тасымалдағышқа қол жеткізу стандартты зауыттық құпия сөзбен қорғалған, ол Кілттік тасымалдағышты беру кезінде айтылады және ЭСҚ Кілттік тасымалдағышқа сақтаудың бірінші әрекеті кезінде Клиент құпия сөзді өзгертуге міндетті, кейіннен құпия сөзді Клиент дербес өзгерте алады;
- a e-Token PASS time based құрылғысын және Кілттік тасымалдағышты беру осы Қосымша келісімнің ажыратылмас бөлігі болып табылатын "Кілттік тасымалдағышты қабылдау-беру актісіне" Тараптардың қол қоюымен сүйемелденеді. Бір Кілттік тасымалдағышта ЭСҚ бір иесінің жабық кілті (құпия кілт) сақталады;

7.3. Егер тексеру кезінде бұл қолдар сенімді деп танылса және құжатты қабылдау кезінде құжатқа қол қойған тұлғаның өзінің жеке кілтінің немесе бағдарламалық жасақтаманың жария болғаны туралы ресми өтініші тіркелмесе, олардың атынан қол қойылған ЭСҚ, ашық (жария) кілттердің тиісті

6.9. Банк не несет ответственности за ущерб, возникший вследствие неправильного оформления Клиентом платежных документов (ошибочные реквизиты, двойные проводки, неправильный адрес получателя платежа и т.д., и т.п.), а также за ошибки, отказ или задержки, происходящие по вине лиц, в пользу которого платит Клиент;

6.10. Банк не несет ответственности за ущерб, возникший вследствие разглашения Клиентом собственного пароля или передачи, вне зависимости от причин, третьим лицам ключевой информации, используемой для шифрования данных.

6.11. Банк не несет ответственности за убытки, понесенные Клиентом в результате любых действий третьих лиц, включая, но, не ограничиваясь, контрагентов Клиента, которым по любым основаниям стали доступны Логин/Пароль, e-Token PASS time based и (или) ключи, если это стало возможным по неосторожности, в том числе включая небрежность, или умысел Клиента, в том числе при неиспользовании Клиентом всех мер безопасности, установленных и согласованных Сторонами настоящего Дополнительного соглашения, с учетом всех приложений к нему.

7. Особые условия

7.1. Стороны настоящего Соглашения, безусловно и безотзывно подтверждают и согласны с тем, что Клиент обязан использовать все средства защиты от несанкционированных платежей (доступов в ДБО), согласованные Сторонами Соглашения, а Банк использовать средства защиты, установленные внутренними нормативными документами Банка и законодательством Республики Казахстан. При этом, Клиент понимает, что обязанности Банка ограничиваются соблюдением положений Соглашения о средствах защиты; и что доступ от имени Клиента к счетам Клиента, допущенный по неосторожности, по вине либо без таковой самого Клиента, либо третьих лиц (в том числе работников Клиента), в результате которого произведен платеж (доступ в ДБО), будет безусловно считаться санкционированным со стороны Клиента. Со своей Стороны Банк обязуется соблюдать условия и применять указанные средства защиты при получении каждого и любого электронного документа (платежного документа), поступившего в Банк от имени / со стороны Клиента.

7.2.Клиентом в обязательном порядке используется Ключевой носитель или e-Token PASS time based

- Ключевой носитель и устройство e-Token PASS time based выдается Банком непосредственно Клиенту/уполномоченному представителю Клиента. Доступ к Ключевому носителю защищен стандартным заводским паролем, который озвучивается при выдаче Ключевого носителя, и при первой попытке сохранения ЭЦП на Ключевой носитель Клиент обязан изменить пароль, в последующем пароль может изменяться Клиентом самостоятельно;

тізімінде немесе e-Token PASS time based құрылғысында тіркелген Тіркеу куәліктері – электрондық құжаттардан туындайтын барлық міндеттемелерді Клиент пен Банк өзара толық көлемде қабылдауға міндеттенеді.
7.4. Тараптардың кез келгені осы Келісімнің 8.3-тармағында қарастырылған талаптарды орындамауы екінші Тараптың бастамасы бойынша осы Келісімді біржақты тәртіппен бұзуға негіздеме болады.
7.5. Клиент ҚБҚ-ғы Клиенттің Жұмыс орнының ақпараттық қауіпсіздігін қамтамасыз ету талаптары мен ұсыныстарын толық көлемде сақтауға міндеттенеді.
7.6. Банкке Келісім бойынша тиесілі комиссиялық сыйақыны Клиенттің Банкте ашылған өзге шоттарынан акцептсіз тәртіпте тікелей дебеттеу арқылы есептен шығару құқығын Банкке береді және бұнымен келіседі.,

8. Дауларды шешу тәртібі

8.1. Тараптар арасында ЭСҚ немесе e-Token PASS time based құрылғысын қолданумен байланысты туындаған дауларды шешуді әрбір нақты дауды шешу үшін құрылған Сараптау-техникалық комиссиясы (бұдан әрі - Комиссия) іске асырады.
8.2. Клиент Банкке Банк Клиент шоты бойынша операцияны орындаған ЭСҚ немесе e-Token PASS time based құрылғысы электронды құжатқа нұсқау көрсетумен наразылық мәннен тұратын өтініш береді. Банктің Клиент өтініш берген күннен бастап 14 (он төрт) жұмыс күнінен аспайтын мерзім ішінде өтінішті қарастыру үшін Комиссия құруға құқығы бар. Комиссия құрамына Клиент өкілдері, Банк өкілдері және қажет болғанда – ҚБҚ-ны шығарушы фирма өкілі, тәуелсіз сарапшылар енгізіледі. Комиссия жұмысы үшін жоғарыда келтірілген тізімнен кемінде үш өкілд қатысуы қажет.
8.3. Комиссия Клиент өтінішін Клиенттің ашық кілт (жария кілт) ЭСҚ немесе e-Token PASS time based құрылғысына және мынадай сатылардан тұратын даулы электрондық құжатты техникалық сараптама жасау арқылы қарастырады:
- операция жүргізу уақыты белгіленеді;
- бақылау сомасын есептеу және оны эталондықпен салыстыру арқылы Тараптардың екеуінің де ҚБҚ бағдарламалық жасақтамаларының тұтастығын тексереді;
- ашық (жария) кілттің немесе e-Token PASS time based құрылғысының Клиентке тиесілігін және құжатты ресімдеу сәтінде әрекет ететінін тексеру іске асырылады;
- e-Token PASS time based құрылғысының немесе ашық (жария) кілттің түпнұсқалығы осы кілттің Клиенттің қойылған қолымен куәландырылған,осы кілттің басып шығарылған түрімен салыстыру арқылы тексеріледі;
- ұсынылған e-Token PASS time based құрылғысын немесе Кілттік тасымалдағышты пайдаланумен

- передача устройства e-Token PASS time based и Ключевого носителя и сопровождается подписанием уполномоченными представителями Сторон «Акта приема-передачи Ключевого носителя», являющегося неотъемлемой частью настоящего Дополнительного соглашения. На одном Ключевом носителе хранятся закрытый ключ (секретный ключ) одного владельца ЭЦП;
7.3. Клиент и Банк взаимно обязуются принимать на себя в полном объеме все обязательства, вытекающие из электронных документов, подписанных от их имени ЭЦП, Регистрационные свидетельства которых зарегистрированы в соответствующем списке открытых (публичных) ключей или устройством e-Token PASS time based, если при проверке эти подписи признаются достоверными и к моменту приема документа не было зафиксировано официального заявления, подписавшего документ лица о компрометации своего личного ключа или программного обеспечения.
7.4. Невыполнение любой из Сторон условия, предусмотренного пункте 8.3. настоящего Соглашения является основанием для расторжения Соглашения по инициативе другой Стороны в одностороннем порядке.
7.5. Клиент обязуется в полном объеме соблюдать условия требования и рекомендации по обеспечению информационной безопасности Рабочего места Клиента в ДБО».
7.6. Клиент соглашается и предоставляет право Банку в безакцептном порядке, путем прямого дебетования, списывать со Счета (-ов) Клиента, иных счетов Клиента, открытых в Банке, комиссионное вознаграждение, причитающееся Банку по Соглашению.

8. Порядок разрешения споров

8.1. Разрешение возникших между Сторонами споров, связанных с применением ЭЦП или устройством e-Token PASS time based, осуществляется создаваемой для разрешения каждого конкретного спорного случая Экспертно-технической комиссией (далее – Комиссия).
8.2. Клиент представляет Банку заявление, содержащее сущность претензии с указанием на электронный документ с ЭЦП или или устройством e-Token PASS time based, на основании которого Банк выполнил операции по счёту Клиента. Банк имеет право в течение не более 14 (четырнадцати) рабочих дней от даты подачи заявления Клиента сформировать Комиссию для рассмотрения заявления. В состав комиссии включаются представители Клиента, представители Банка и при необходимости – представитель фирмы-разработчика ДБО, независимые эксперты. Для работы Комиссии необходимо присутствие не менее трех представителей из вышеприведенного списка.
8.3. Комиссия проводит рассмотрение заявления Клиента путем технической экспертизы открытого ключа (публичного ключа) ЭЦП или или

құрылғылардың жұмысқа жарамдылығын тексеру үшін 1 теңге сомасына тесттік операция жүргізіледі. Деректер базасынан тесттік операциялар шығарылады, ол бойынша e-Token PASS time based құрылғысының түпнұсқалығы және ЭСҚ дұрыстығы мен түпнұсқалығы тексеріледі;

- Жүйенің деректер базасы мұрағатынан дауланатын операциялардың e-Token PASS time based немесе ЭСҚ деректері шығарылады және электронды қол орындалуының түпнұсқалығы тексеріледі.

Техникалық сараптама мәліметтері негізінде Акт жасалады, оған сараптама жүргізуге қатысқан Комиссия құрамы қол қояды. Клиент өкілі Комиссия құрамына қатысудан бас тартқан жағдайда көрсетілген Актіде Клиенттің қатысудан бас тартқаны туралы белгі қойылады.

8.4. Тараптар Комиссия шешімдерін қабылдаған жағдайда ол келесі жұмыс күнінен кешіктірілмей орындалуы тиіс.

8.5. Комиссия шешімін орындаудан бас тартқан жағдайда Тараптар араларында туған дауды Қазақстан Республикасының заңнамасына сәкйес сот органдарының қарастыруына береді.

9. Қорытынды ережелер

9.1. Келісім Шот шарттың ажыратылмас бөлігі болып табылады, Тараптар қол қойған және Клиент ҚБҚ-қа қосқаны үшін комиссияны төлеген күннен бастап күшіне енеді. Келісім егер Тараптар қосымша түрде өзге мерзімді келісімдемесе, Шот шарты әрекет ететін мерзімде қолданылады.

Қосымша келісімге қосымшалар:

1) №1 қосымша. ҚБҚ-ғы Клиенттің Жұмыс орнын ақпараттық қауіпсіздікпен қамту жөніндегі талаптар мен ұсынымдар
2) №2 қосымша Беру-қабылдау-актісі;
3) №3 қосымша. Интернет-Клиент/Банк-Клиент модулінде пайдаланушыларды тіркеуге / өзгертуге өтініш.
4) №4 қосымша Деректемелерді ауыстыруға өтініш
5) №5 қосымша ҚБҚ-да пайдаланушыны өшіруге /оқшаулауға өтініш
6) №6 қосымша ҚБҚ-ға орнату актісі

Осы Келісімнің барлық қосымшалары тиісті түрде ресімделген, Келісімнің ажыратылмас бөліктері болып табылады.

10. Тараптардың мекенжайлары мен қолдары

устройством e-Token PASS time based Клиента и оспариваемого электронного документа, включающей следующие этапы:

- устанавливается время проведения операции;
- проверяется целостность программного обеспечения ДБО обоих Сторон, путем вычисления контрольной суммы и ее сравнения с эталонной;
- осуществляется проверка принадлежности открытого (публичного) ключа или устройства e-Token PASS time based Клиенту и его действенность в момент оформления документа;
- проверяется подлинность устройства e-Token PASS time based или открытого (публичного) ключа путем сравнения его с распечаткой этого ключа, заверенной физической подписью Клиента;
- проводится тестовая операция на сумму 1 тенге с использованием предъявленного устройства e-Token PASS time based или Ключевого носителя для проверки работоспособности устройств. Из базы данных извлекаются данные по тестовой операции, по которым проверяется подлинность устройство e-Token PASS time based или правильность и подлинность ЭЦП;
- извлекаются данные e-Token PASS time based или ЭЦП оспариваемой операции из архива базы данных ДБО, и проверяется подлинность выполнения электронной подписи.

На основании данных технической экспертизы составляется Акт, который подписывается составом Комиссии, принявшим участие в проведении экспертизы. В случае отказа представителя Клиента участвовать в составе Комиссии, в указанном Акте делается отметка об отказе Клиента от участия.

8.4. В случае принятия Сторонами решения Комиссии, оно должно быть выполнено не позднее следующего рабочего дня.

8.5. В случае отказа от исполнения решения Комиссии, Стороны передают возникший между ними спор на рассмотрение в судебные органы в соответствии с законодательством Республики Казахстан

9. Заключительные положения

9.1. Соглашение является неотъемлемой частью Договора счета, вступает в силу со дня его подписания Сторонами и оплаты Клиентом комиссии за подключение к ДБО. Соглашение действует в течение всего срока действия Договора счета, если иной срок не будет согласован Сторонами дополнительно.

Приложения к Дополнительному соглашению:

1) Приложение №1 Требования и рекомендации по обеспечению информационной безопасности
   Рабочего места Клиента в ДБО;
2) Приложение №2Акт приема-передачи;
3) Приложение № 3 Заявление на регистрацию /изменение Пользователей в модуле Интернет-Клиент/Банк-Клиент

4) Приложение №4 Заявление на смену реквизитов
5) Приложение №5 Заявление на отключение/блокировку пользователя в ДБО
6) Приложение №6 Акт установки в ДБО

Все приложения к настоящему Соглашению оформленные надлежащим образом, являются неотъемлемыми частями Соглашения.

10. Адреса и подписи Сторон

«Банк»: 050002, Республика Казахстан/050002, Қазақстан Республикасы
г. Алматы, ул. Кунаева, 56 / Алматы қ., Қонаев к-сі 56
Коршот: KZ67125KZT1001300285 в Управлении учета монетарных операций (ООКСП) НБ РК /
ҚР ҰБ Монетарлық операцияларды есепке алу басқармасындағы (КШТҚКБ) коршот: KZ67125KZT1001300285
БИН/ БСН: 950240000112
БИК/ БСК: EURIKZKA
ОКПО/ КҰЖК: 30521653
SWIFT: EURI KZ KA

Подпись/ Қолы _____
М.П./ М.О.
Дата/ Күні: ____/_____/_____

«Клиент»:
Наименование организации/ Ұйымның атауы: _____
Адрес/ Мекенжайы: _____
БИН/ БСН_____
Тел/факс: _____
Номер счета/ Шот нөмірі: _____
Эл. Мекенжайы/ Эл. мекенжайы: _____
Ф.И.О./Т.А.Ә.:_____
Должность / Лауазымы: _____

Подпись/ Қолы _____
М.П./ М.О.
Дата/ Күні: ____/_____/_____
_____/_____/
Қолы
20___ж. «_____»_____

20___ жылғы _____№___ ағымдағы банктік шот шартына
№_____ қосымша келісімге
№1 қосымша

(заңды тұлғалар, жеке кәсіпкерлер, шаруа немесе фермер қожалықтары, жеке нотариустер (жалпы шаруашылық мақсаттар), жеке сот орындаушылар (жалпы шаруашылық мақсаттар) және адвокаттар үшін)

Клиенттің ҚБҚ-ғы
Жұмыс орнының ақпараттық қауіпсіздігін қамтамасыз ету бойынша талаптар мен ұсынымдар

1. Жалпы ереже

1.1. « WEB ақпараттық қауіпсіздігі – ҚБҚ интерфейсі кешенді (ұйымдастырушылық, әкімшілік, техникалық және бағдарламалық) шаралармен және құралдармен қамтамасыз етілуі тиіс.

1.2. Ақпараттың қауіпсіздігін қамтамасыз ету мақсатында.

- КЛИЕНТТІҢ басшылығымен ҚБҚ-де жұмыс істеуге рұқсат етілетін пайдаланушылар мен әкімшілердің тізімі әрбір пайдаланушыға нақты функциялар мен өкілеттіктер бекітумен бекітілуі тиіс.
- КЛИЕНТТІҢ басшылығымен ҚБҚ қауіпсіздігін қамтамасыз ету үшін жауапты қызметкер тағайындалуы тиіс.
- ҚБҚ пайдаланушылары ҚБҚ-ның құжаттамасына және осы әдістемелік ұсынымдарға сәйкес пайдалану ережелерімен таныстырылуы тиіс.
- ҚБҚ-ға кіруге арналған мәліметтер мен кілттік ақпаратты тасымалдағыштар санкцияланбаған қол жеткізуден (СҚЖ) қорғалуы тиіс.

1.3. ЭСҚ жабық (құпия) кілттерін сақтауға арналған қорғалған USB-токен тасымалдағыштарды пайдалану құпия кілттерді көшіруден қорғайды, бірақ айтылған талаптарды орындаудан босатпайды.

1.4. Қауіпсіз ортаны қамтамасыз ету үшін Клиентке өз компьютерінде мыналарды жасау керек:

- .exe .cmd .bat .dll ықтимал қауіпті жүктеулерді оқшаулайтын электронды хаттарды сүзгілеу үшін БЖ орнату.
- Туындаған қателерді, пайдаланушылардың кіруін және бағдарламаларды іске қосуды тіркейтін оқиғалардың жүйелі аудитін қосу, журналды кезеңділікпен қарап тұру және қателерге назар аудару.
- Компьютерге вирус енгеніне күдік туындаған жағдайда жұмыс станцияларын тексеру.

2. ҚБҚ-ны рұқсат етілмеген қолжетімділіктен (РЕҚ) қорғау бойынша талаптар

2.1. ҚБҚ-ға кіруге арналған мәліметтер мен кілттік ақпаратты тасымалдағыштар рұқсат етілмеген қолжетімділіктен (СҚЖ) қорғау мыналардың мүмкіндігін болдырмау мақсатында іске асырылады:

- ҚБҚ құралдары орнатылған компьютерлерде компьютерлік вирустардың және ҚБҚ-ның БЖ бұзуға, жұмысқа жарамдылығын бұзуға және жаңартуға немесе ақпаратты алып алуға бағытталған бағдарламалардың пайда болуы;
- ҚБҚ-ның техникалық және бағдарламалық құралдарына, сондай-ақ олардың құрамына рұқсат етілмеген өзгерістер енгізу;
- Электронды құжатқа (ЭҚ) рұқсат етілмеген өзгерістер енгізу;

2.2. ҚБҚ-ны жеке, осы мақсаттар үшін арнайын бөлінген дербес компьютерде пайдалану ұсынылады. **Бұл компьютер желілік шабуылдар мен вирусқа қарсы қорғауларда міндетті түрде қорғалуы тиіс.**

2.3. ҚБҚ-ны санкцияланбаған қол жеткізуден қорғау мақсатында компьютерлерге рұқсат етілмеген қол жеткізуден қорғаудың бағдарламалық-аппараттық кешенін орнатуға ұсыныс жасалады.

2.4. РЕҚ қорғау кешінінің көмегімен ҚБҚ-ның тұтастығын бақылауды қамтамасыз ететін және пайдаланушыларға берілетін мүмкіндіктер мен өкілеттіктер шеңберінде қатаң жұмыс істеуге рұқсат берілетін функционалдық тұйық орта қалыптастыру ұсынылады. Жүйелік және жүктеу файлдары, сондай-ақ ақпаратты криптографиялық қорғау құралымен (АККҚ) істелетін жұмыстармен байланысты файлдар қорғалуы тиіс.

2.5. ҚБҚ-мен жұмыс істеу үшін пайдаланылатын дербес компьютерде БЖ әзірлеу құралдары және ретке келтіру орнатылуы тиіс емес.

2.6. ҚБҚ-мен жұмыс істеу үшін пайдаланылатын дербес компьютерлердің жүйе блогын рұқсатсыз ашуға кедергі болатын шаралар қабылдаған жөн.

2.7. РЕҚ қорғаудың бағдармалық-ақпараттық құралы әкімшісінің құқығы ҚБҚ қауіпсіздігін қамтамасыз етуге жауапты қызметкерге беріледі. Көрсетілген қызметкер ЭҚ қабылдау-беруге, ЭҚ құрастыруға және кілттік ақпаратты тасымалдағыштарды пайдалануға қатысатын ҚБҚ-ның әрбір қатысушысы үшін қол жеткізу құқығын құрастырады.

2.8. Сондай-ақ компьютерлерді РЕҚ қорғау үшін операциялық жүйенің штаттық мүмкіндіктері пайдаланылуы тиіс.

3. Кілттік ақпаратты тасымалдағыштарды сақтау және пайдалану бойынша талаптар

3.1. Клиент жабық (құпия) криптографиялық кілттерді дербес түрлендіруге тиіс.

3.2. Кілттік ақпаратты тасымалдағыштар олар тиесілі тұлғаларда ғана сақталуы тиіс.

3.3. Құпия кілттер бар кілттік ақпаратты тасымалдағыштарды сақтау және пайдалану тәртібі оларға санкцияланбай қол жеткізуді болдырмауға тиіс.

3.4. Кілттік ақпаратты тасымалдағыштарға қол жеткізуі бар тұлғалар тізімі КЛИЕНТ басшылығының бұйрығымен немесе өкімімен оларға бекітілген функциялармен өкілдіктерге сәйкес анықталады.

3.5. Кілттік ақпаратты тасымалдағыштармен жұмыс жүргізу уақытында оларға бөгде тұлғалардың қолжетімділігі болмауы тиіс.

3.6. Кілттік ақпаратты тасымалдағыштарды сақтау үшін сенімді металл сейфтер орнатылады.
3.7. Жұмыс күні аяқталғанда, сондай-ақ сеанстардың Банктермен уақытынан тыс байланыс кезінде Кілттік ақпаратты тасымалдағыштар сейфте сақталуы тиіс.
3.8. Кілттік ақпаратты тасымалдағыштарды басқа құжаттармен бір сейфте сақтауға рұқсат етіледі, бұл ретте оларға бөгде адамдардың жасырын қолжетімділігі мүмкіндігін болдырмайтындай бөлек орауда сақталуы тиіс.
3.9. Келесілерге рұқсат етілмейді:

- кілттік ақпаратты тасымалдағыштарды рұқсат етілмеген тұлғаларға беру;
- құпия кілттерді дисплейге немесе принтерге шығару;
- кілттік ақпаратты тасымалдағыштарды ҚБҚ-ның қызмет етуімен қарастырылмаған режимдерде компьютердің оқитын құрылғысына, сондай-ақ басқа компьютерлердің оқитын құрылғыларына қою;
- кілттік ақпаратты тасымалдағышты жұмыс орнында қараусыз қалдыру;
- кілттік ақпаратты тасымалдағышқа бөгде файлдар жазу.

4. ҚБҚ-ны рұқсат етілмеген қолжетімділіктен қорғау бойынша тәжірибелік ұсынымдар.

4.1. ҚБҚ-ға желілік қол жеткізуді (оның ішінде желіге қашықтан ену) жергілікті желінің басқа жұмыс станцияларынан және әсіресе сыртқы желілерден толық оқшаулау ұсынылады. Осы мақсатпен желі аралық дербес экранды тиісті түрде орнату және баптау.
4.2. ҚБҚ пайдаланушыларыға Интернет желісін пайдалануды шектеуге ұсыныс жасалады, яғни біріктіруге арналған мекенжайларға қолжетімділік тізімін шектеу, банк серверімен біріктіруге ғана рұқсат беру. Осы мақсатпен бәрінен бұрын орнатылған желі аралық дербес экранды пайдаланған дұрыс.
4.3. Вирусқа қарсы бағадарламалық жасақтама міндетті түрде орнатылуы және үнемі жаңартылуы тиіс. Қауіпсіздік саясатының ең жоғарғы деңгейін бастапқы қалпында орнатуға ұсыныс жасалады, яғни вирустар тапқанда пайдаланушылар жауабын талап етпейтін.
4.4. Жүйемен жұмыс істейтін ҚБҚ пайдаланушыларының компьютерде бағдарламалық жасақтаманың осы есептік жазуларымен орнату мүмкнідігін шектеу мақсатында әкімші құқығы жоқ болуы тиіс. Компьютердің файлдық ресурстарына, әсіресе жазуларға қол жеткізу ең аз қажетті құқықтармен шектелуі тиіс. Пайдаланушылар рұқсат берілген қосымшаларды ғана іске қосулары тиіс.
4.5. ҚБҚ пайдаланушылар міндетті түрде қауіпсіздіктің негізгі талаптарын сақтау мәселелері және әсіресе вирусқа қарсы бағдарламаларды пайдалану мәселелері бойынша нұсқамалықтан өтулері тиіс.
4.6. Жергілікті (немесе домендік) саясатта компьютерде операциялық жүйеге кіру мүмкіндігі бар пайдаланушылар тізімін шектеуге ұсыныс жасалады.
4.7. Сыртқы электронды почтаны (Интернет желісінен) қабылдауды шектеу немесе толығымен бас тарту ұсынылады. Алынатын почта міндетті түрде вирусқа қарсы құралдармен тексерілуі тиіс.
4.8. Компьютерде бір ғана НЖ орнатылуы тиіс.
4.9. Средствами BIOS компьютер құралдарымен қатты дискте орнатылғаннан ерекшеленетін операциялық жүйені жүктеу мүмкіндігін алып тастау ұсынылады, яғни дискеттен, CD/DVD жетектерден, USB flash дисктерден жүктеуді, желілік жүктеуді және т.б. ажырату.
4.10. BIOS баптауларын өзгертуге қолжетімділік құпия сөзбен қорғалуы тиіс.
4.11. Операциялық жүйе пайдаланушыларына құпия сөздер белгіленуі тиіс. Құпия сөздердің ұзындығы алты белгіден кем болмауы тиіс. Құпия сөдердің әрекет ету мерзімі шектелген болуы тиіс.
4.12. Компьютердің жүйе блогына оны рұқсатсыз ашуды болдырмау үшін сүргі салу ұсынылады.
4.13. Компьютерге қолжетімділікті шектеу, пайдаланылатын БЖ тұтастығын тексеру үшін компьютерге РЕҚ қорғаудың бағдарламалық-ақпараттық кешенін орнату және баптау ұсынылады («Аккорд», «Соболь» және т.б.).
4.14. Кілттерді тек жеке алынатын ақпарат тасымалдағыштарда ғана сақтауға және оларды басқа мақсатқа пайдаланбауға ұсыныс жасалады. Тасымалдағыштарды дисководтарға тек ҚБҚ-мен тікелей жұмыс кезінде Банктің қол қою немесе айырбастау операцияларын орындау сәттерінде ғана салу керек, операция аяқталғаннан кейін бұл тасымалдағышты шығарып алу қажет. Кілттік ақпарат бар тасымалдағыштарды басқа компьютерлерге қоспаңыз.
4.15. Компьютерге сыртқы қондырғыларды, оның ішінде өндірістік қажеттілікпен қарастырылмаған ақпарат тасымалдағыштарды қосу ұсынылмайды.

5. АКҚҚ есепке алу бойынша жалпы талаптар

5.1. АКҚҚ және олардың кілттік тасымалдағыштарын даналап есепке алу журналын жүргізу қажет.
5.2. Құпия кілттерді жою кілттік тасымалдағышты олар орналасқан жерде табиғи жою немесе кілттік тасымалдағышты бүлдірмей (оны көп мәрте пайдалану мүмкіндігін қамтамасыз ету үшін) өшіру арқылы жүргізіледі.
5.3. Кілттер жоспарлы ауыстырылғаннан немесе кілттері жария болып қалғаннан кейін АКҚҚ пайдаланушылар әрекеттен шығарылған шифрлаудың құпия кілттерін және ЭСҚ барлық магнитті тасымалдағыштардан кілттерді әрекеттен шығарған сәттен кейін он күннен кешіктірмей жояды. Кілттерді жою туралы Есепке алу журналында тиісті жазу жазылады.

Клиент _____

Т.А.Ә. /лауазымы_____

ТАНЫСТЫ:_____ Қолы Күні: ____/_____/_____

Приложение №1
К Дополнительному соглашению №__
к Договору текущего банковского счета №_____ от _____ 20___ года

(для юридических лиц, индивидуальных предпринимателей, крестьянских или фермерских хозяйств, частных нотариусов (общехозяйственные цели), частных судебных исполнителей (общехозяйственные цели) и адвокатов) к Дополнительному

Требования и рекомендации по обеспечению информационной безопасности Рабочего места Клиента в ДБО

6. Общие положения

6.1. «Информационная безопасность WEB – интерфейса ДБО должна обеспечиваться комплексными (организационными, административными, техническими и программными) мерами и средствами.

6.2. С целью обеспечения безопасности информации:

- руководством КЛИЕНТА должен быть утвержден список пользователей и администраторов, допускаемых к работе в ДБО, с закреплением за каждым пользователем конкретных функций и полномочий;
- руководством КЛИЕНТА должен быть назначен сотрудник ответственный за обеспечение безопасности ДБО;
- пользователи ДБО должны быть ознакомлены с правилами эксплуатации согласно документации к ДБО и с настоящими методическими рекомендациями;
- данные для входа в ДБО и носители ключевой информации должны быть защищены от несанкционированного доступа (НСД).

6.3. Использование защищенного носителя USB-токен для хранения закрытых (секретных) ключей ЭЦП защищает секретные ключи от копирования, но не освобождает от выполнения изложенных требований.

6.4. Для обеспечения безопасной среды на своем компьютере Клиентну надлежит. :

- УстановитьПО для фильтрации электронных писем, блокирующее потенциально опасные вложения .exe .cmd .bat .dll
- Включить системный аудит событий, регистрирующий возникающие ошибки, вход пользователей и запуск программ, периодически просматривать журнал и реагировать на ошибки.
- Проверять рабочие станции в случае подозрения заражения компьютера вирусом.

7. Требования по защите ДБО от несанкционированного доступа (НСД)

7.1. Защита данных для входа в ДБО и носителей ключевой информации от несанкционированного доступа осуществляется с целью исключения возможностей:

- появления в компьютерах, на которых установлены средства ДБО, компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию ПО ДБО, либо на перехват информации;
- внесения несанкционированных изменений в технические и программные средства ДБОы, а также в их состав;
- внесения несанкционированных изменений в Электронный документ (ЭД).

7.2. ДБО рекомендуется использовать на отдельном, специально выделенном для этих целей персональном компьютере. **Должна быть обеспечена в обязательном порядке защита данного компьютера от сетевых атак и антивирусная защита.**

7.3. В целях защиты ДБО от несанкционированного доступа на компьютеры рекомендуется установить программно-аппаратный комплекс защиты от несанкционированного доступа.

7.4. Рекомендуется сформировать с помощью комплекса защиты от НСД функционально замкнутую среду, обеспечивающую контроль целостности ДБО и допускающую работу пользователей строго в рамках, предоставляемых им возможностей и полномочий. Защите подлежат системные и загрузочные файлы, а также файлы, связанные с работой средств криптографической защиты информации (СКЗИ).

7.5. На персональном комьпютере, используемом для работы с ДБОой не должны устанавливаться средства разработки ПО и отладчики.

7.6. Следует принять меры, препятствующие несанкционированному вскрытию системных блоков персональных компьютеров, используемых для работы с ДБО.

7.7. Права администратора программно-аппаратных средств защиты от НСД предоставляются сотруднику, ответственному за обеспечение безопасности ДБО. Указанный сотрудник формирует права доступа для каждого пользователя ДБО, участвующего в приеме-передаче ЭД, формировании ЭД и использовании носителей ключевой информации.

7.8. Для защиты компьютеров от НСД также должны использоваться штатные возможности операционной системы.

8. Требования по организации хранения и использования носителей ключевой информации

8.1. Клиент должен самостоятельно генерировать закрытые (секретные) криптографические ключи.

8.2. Носители ключевой информации должны храниться только у тех лиц, которым они принадлежат.

8.3. Порядок хранения и использования носителей ключевой информации с секретными ключами должен исключать возможность несанкционированного доступа к ним.

8.4. Список лиц, имеющих доступ к носителям ключевой информации, определяется приказом или распоряжением руководства КЛИЕНТА, согласно закрепленными за ними функциями и полномочиями.

8.5. Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

8.6. Для хранения носителей ключевой информации должны устанавливаться надежные металлические сейфы.
8.7. По окончании рабочего дня, а также вне времени сеансов связи с Банком носители ключевой информации должны храниться в сейфе.
8.8. Хранение носителей ключевой информации допускается в одном сейфе с другими документами, при этом отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.
8.9. Не разрешается:

- передавать носители ключевой информации лицам, к ним не допущенным;
- выводить секретные ключи на дисплей или принтер;
- вставлять носитель ключевой информации в считывающее устройство компьютера в режимах, не предусмотренных функционированием ДБО, а также в считывающие устройства других компьютеров;
- оставлять носитель ключевой информации без присмотра на рабочем месте;
- записывать на носитель ключевой информации посторонние файлы.

9. Практические рекомендации по защите ДБО от несанкционированного доступа

9.1. Рекомендуется полностью блокировать сетевой доступ к ДБО (в том числе и удаленный вход в сеть) с других рабочих станций локальной сети и в особенности из внешних сетей. С этой целью рекомендуется установить и настроить соответствующим образом персональный межсетевой экран.
9.2. Рекомендуется ограничить использование сети Интернет пользователями ДБО, т.е. ограничить список доступных для соединения адресов, например, разрешить только соединение с сервером банка. С этой целью также лучше всего использовать установленный персональный межсетевой экран.
9.3. В обязательном порядке должно быть установлено и регулярно обновляться антивирусное программное обеспечение. Рекомендуется установить по умолчанию максимальный уровень политик безопасности, т.е. не требующий ответов пользователя при обнаружении вирусов.
9.4. Пользователи ДБО, работающие с системой не должны иметь прав администратора, с целью ограничения возможностей установки под этими учетными записями программного обеспечения на компьютере. Доступ к файловым ресурсам компьютера, особенно на запись, должен быть ограничен минимально необходимыми правами. Пользователи должны запускать только те приложения, которые им разрешены.
9.5. Пользователи ДБО, должны быть в обязательном порядке проинструктированы по вопросам соблюдения основных требований безопасности, и в особенности по вопросам использования антивирусных программ.
9.6. Локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.
9.7. Рекомендуется ограничить или полностью отказаться от приема внешней (из Сети Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами.
9.8. На компьютере должна быть установлена только одна ОС.
9.9. Средствами BIOS компьютера следует исключить возможность загрузки операционной системы, отличной от установленной на жестком диске, т.е. отключить загрузку с дискет, CD/DVD приводов, USB flash дисков, сетевую загрузку и т.п.
9.10. Доступ к изменению настроек BIOS должен быть защищен паролем.
9.11. Пользователям операционной системы должны быть назначены пароли. Длина паролей должна составлять не менее шести символов. Срок действия паролей должен быть ограничен.
9.12. Рекомендуется опечатать системный блок компьютера для предотвращения его несанкционированного вскрытия.
9.13. Для ограничения доступа к компьютеру, проверки целостности используемого ПО, рекомендуется установить и настроить на компьютер программно-аппаратный комплекс защиты от НСД («Аккорд», «Соболь» и т.п.).
9.14. Рекомендуется хранить ключи только на отдельных съемных носителях информации, и не использовать их для других целей. Вставлять носители в дисководы только непосредственно при работе с ДБО в моменты выполнения операций подписания или обмена с Банком, по завершении операции необходимо извлечь данный носитель. Не подключайте носители с ключевой информаций к другим компьютерам.
9.15. Не рекомендуется подключать к компьютеру внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

10. Общие требования по учету СКЗИ

10.1. Необходимо вести Журнал поэкземплярного учета СКЗИ и ключевых носителей к ним.
10.2. Уничтожение секретных ключей может производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания без повреждения ключевого носителя (для обеспечения возможности его многократного использования).
10.3. После плановой смены ключей или компрометации ключей пользователи СКЗИ уничтожают выведенные из действия секретные ключи шифрования и ЭЦП со всех магнитных носителей не позднее чем через десять дней после момента вывода ключей из действия. Об уничтожении ключей делается соответствующая запись в Журнале учета.

Клиент _____

Ф.И.О. /должность_____

ОЗНАКОМЛЕН:_____ Подпись Дата: ____/_____/_____

20___ жылғы _____№___ ағымдағы банктік шот шартына
№_____ қосымша келісімге
№2 қосымша

(заңды тұлғалар, жеке кәсіпкерлер, шаруа немесе фермер қожалықтары, жеке нотариустер (жалпы шаруашылық мақсаттар), жеке сот орындаушылар (жалпы шаруашылық мақсаттар) және адвокаттар үшін)

Приложение №2
К Дополнительному соглашению №__
к Договору текущего банковского счета №_____ от _____ 20___ года

(для юридических лиц, индивидуальных предпринимателей, крестьянских или фермерских хозяйств, частных нотариусов (общехозяйственные цели), частных судебных исполнителей (общехозяйственные цели) и адвокатов)к Дополнительному

Еуразиялық Банк

АКТ передачи-приема / Беру-қабылдау актісі
№ _____

г. _____ қ. 20__ ж. «___»_____

АО «Евразийский Банк», именуемый в дальнейшем Банк передал, а Клиент принял: / «Еуразиялық Банк» АҚ, бұдан әрі Банк деп аталады, тапсырды, ал Клиент қабылдады:

Вид/ түрі	**Серийный номер / Сериялық нөмірі**	**Количество/Саны**	**ФИО пользователей / Пайдаланушылардың ТАӘ**	**Должность пользователей / Пайдаланушылардың лауазымы**
Ключевой носитель /Кілттік тасымалдаушы				
ПИН-конверт УЦ/КО-тың ПИН-конверті				
Устройство e-Token PASS time based (e-Token PASS event based)/ e-Token PASS time based (e-Token PASS event based)құрылғысы				

дополнительные поля при необходимости добавить вручную / қажеттілік болғанда қосымша жолақтарды қолмен қосу қажет

Настоящий Акт является неотъемлемой частью Соглашения № _____ от «___» _____ 20__ г.
Осы Акт 20__ ж. «___» _____№ _____ келісімнің ажыратылмас бөлігі болып табылады.

«Банк»:
Ф.И.О./ Т.А.Ә.: _____
Должность/ Лауазымы: _____
Подпись/ Қолы _____
М.П. / М.О.

Дата/ Күні: ____/_____/_____

«Клиент»:
Наименование организации/ Ұйымның атауы:
_____
Ф.И.О./ Т.А.Ә.: _____
Должность / Лауазымы: _____
Подпись/ Қолы _____
М.П./ М.О.
Дата/ Күні: ____/_____/_____

20___ жылғы _____№___ ағымдағы банктік шот шартына
№_____ қосымша келісімге
№3 қосымша

(заңды тұлғалар, жеке кәсіпкерлер, шаруа немесе фермер қожалықтары, жеке нотариустер (жалпы шаруашылық мақсаттар), жеке сот орындаушылар (жалпы шаруашылық мақсаттар) және адвокаттар үшін)

Приложение №3
К Дополнительному соглашению №__
к Договору текущего банковского счета №_____ от _____ 20___ года

(для юридических лиц, индивидуальных предпринимателей, крестьянских или фермерских хозяйств, частных нотариусов (общехозяйственные цели), частных судебных исполнителей (общехозяйственные цели) и адвокатов) к Дополнительному

Интернет-Клиент/ Банк-Клиент модулінде пайдаланушыларды тіркеуге / өзгертуге № _____ өтініш
Заявление на регистрацию / изменение Пользователей в модуле Интернет-Клиент/Банк-Клиент № _

г._____ қ. 20__ж./г. «___»_____

Клиенттің толық атауы/ Полное наименование Клиента _____
орналасқан мекенжайы/расположенного по адресу _____
қызмет көрсететілетін филиал (негізгі) / /обслуживающийся в Филиале(основной) _____
E-mail_____телефон___**+7 (__ __ __)__ __ __ __ __ __ __**

☐ **Жаңа пайдаланушы үшін модуль (құпия сөз және логин) дайындау және оған келесі тіркеу куәлігін және (немесе) e-Token PASS байластыру/ Изготовить для нового пользователя модуля (изготовить логин и пароль) и подвязать к нему следующее регистрационное свидетельство и (или) e-Token PASS**

☐ **Жаңа тіркеу куәлігін және (немесе) e-Token PASS модульдің бұрын дайындалған пайдаланушысына байластыру/ Подвязать новое регистрационное свидетельство и (или) e-Token PASS**
к ранее изготовленному пользователю модуля

ТАӘ/ ФИО	Жеке басын куәландырушы құжат/ Д-т уд.личность	ЖСН/ ИИН	E-mail, телефон	Қол қою құқығы/ Право подписи	Тіркеу куәлігінің (сертификаттың) сериялық нөмірі /Серийный номер регистрационного свидетельства (сертификата)	e-Token PASS сериялық нөмірі/серийный номер e-Token PASS	
						e-Token PASS event based	e-Token PASS time based

Интернет-Клиент модулін пайдаланушыны к услуге «Кеңейтілген құқықтар» қызметіне қосуды сұрайды / Просит подключить пользователя модуля Интернет-Клиент к услуге «Расширенные права»

ТАӘ (толығымен)/ ФИО (полностью)	Қол қою құқығы/ Право подписи	Шот/Счет	Құжаттың ең көп сомасы (сомасы көрсетілсін) / Максимальная сумма документа (указать сумму)

дополнительные поля при необходимости добавить вручную/ қажеттілік болғанда қосымша жолақтарды қолмен қосу қажет

«Клиент»:
Т.А.Ә./ Ф.И.О _____
Лауазымы/ Должность _____
Қолы/Подпись _____
М.О../ М.П.
Күні/Дата____/_____/_____

20___ жылғы _____
№___ ағымдағы банктік шот шартына
№___ қосымша келісімге
№4 қосымша

(заңды тұлғалар, жеке кәсіпкерлер, шаруа немесе фермер қожалықтары, жеке нотариустер (жалпы шаруашылық мақсаттар), жеке сот орындаушылар (жалпы шаруашылық мақсаттар) және адвокаттар үшін)

Приложение №-4
К Дополнительному соглашению №__
к Договору текущего банковского счета №_____ от
_____ 20___ года

(для юридических лиц, индивидуальных предпринимателей, крестьянских или фермерских хозяйств, частных нотариусов (общехозяйственные цели), частных судебных исполнителей (общехозяйственные цели) и адвокатов) к Дополнительному

Еуразиялық Банк

№ ___ деректемелерді ауыстыруға өтініш

_____қ. 20__ж. «___»_____

Өтініш беруші_____
(Клиенттің толық атауы)
_____
арқылы _____
негізінде әрекет ететін _____
_____
__ _____ қызмет көрсетіледі
(орны)
осы арқылы ұйымның деректемелерінің өзгертілгені туралы келесі тәртіппен хабарлайды:

Евразийский Банк

Заявление на смену реквизитов
№ _____

г. _____ «___»_____20__г.

Заявитель:_____
(полное наименование Клиента)
_____
в лице
_____
действующий на основании_____
_____
обслуживается в
_____
(место)
настоящим уведомляет об изменении реквизитов организации в следующем порядке:

Ранее действующие реквизиты/ Бұрын қолданылған деректемелер	**Новые реквизиты/ Жаңа деректемелер**
Наименование, юр. форма/ Атауы, заңды нысаны: _____ _____ _____ _____ Месторасположение/ Орналасқан жері: _____ _____ _____; Иное/ Өзге: _____ _____ _____ _____ _____.	Наименование, юр. форма/ Атауы, заңды нысаны: _____ _____ _____ Месторасположение/ Орналасқан жері: _____ _____ _____; Иное/ Өзге: _____ _____ _____ _____

Талап етілген өзгерістерді енгізу бойынша жұмыстар жүргізуді өтінеміз.

Заңды тұлғаның басшысы:
_____
(Т.А.Ә.)
_____
(қолы)
М.О.

Өтініш қабылданды 20___ж. «____»_____:

Просим произвести работы по внесению требуемых изменений.

Руководитель юридического лица:
_____
(Ф.И.О.)
_____
(подпись)
М.П.

Заявление принято «____»_____20___г.:

_____ _____

(Т.А.Ә., лауазымы) (Ф.И.О., должность)

_____ _____

(қолы) (подпись)

Мөртабан Штамп

20___ жылғы _____
№___ ағымдағы банктік шот шартына
№___ қосымша келісімге
№5 қосымша

(заңды тұлғалар, жеке кәсіпкерлер, шаруа немесе фермер қожалықтары, жеке нотариустер (жалпы шаруашылық мақсаттар), жеке сот орындаушылар (жалпы шаруашылық мақсаттар) және адвокаттар үшін)

Приложение №-5
К Дополнительному соглашению №__
к Договору текущего банковского счета №_____ от _____ 20___ года

(для юридических лиц, индивидуальных предпринимателей, крестьянских или фермерских хозяйств, частных нотариусов (общехозяйственные цели), частных судебных исполнителей (общехозяйственные цели) и адвокатов)
к Дополнительному

ҚБҚ-да пайдаланушыны өшіруге /оқшаулауға өтініш
Заявление на отключение/блокировку пользователя в ДБО

Осы арқылы /Настоящим _____
_____
(Клиенттің атауы) / (наименование Клиента)
Заңды мекенжайы/Юридический адрес: _____
_____

Тіркеу куәлігі/Регистрационное свидетельство № _____ от «_____» _____200___ж/г., берілген/выдано _____ _____, арқылы/в лице _____,
негізінде қолданылатын/действующего(-щей) на основании _____,
_____ байланысты/в связи с
(криптопрофильді оқшауландыру себебі)/ (причина блокировки криптопрофиля):
_____

келесі пайдаланушылардың криптопрофилін оқшауландыруды және тіркелу куәлігін (бар болса) қайта қайтаруды өтінеді/просит заблокировать криптопрофиль и отозвать регистрационное свидетельства (при наличии), следующих пользователей:

1._____
(лауазымы, тегі, аты-жөні/ должность, фамилия, имя, отчество)
_____

2. _____
(лауазымы, тегі, аты-жөні/ должность, фамилия, имя, отчество)
_____

3._____
(лауазымы, тегі, аты-жөні/ должность, фамилия, имя, отчество)
_____

Т.А.Ә./Ф.И.О. _____

Лауазымы/Должность _____

Қолы/Подпись _____

Күні/Дата: ____/_____/_____ Уақыты/Время: _____/_____

күн/день ай/месяц жыл/год сағаты/часы минуты/минуты

Өтінішті қабылдаған менеджердің қолы/Подпись Менеджера, принявшего заявление
_____ /_____
(қолы)/(подпись) (тегі, аты-жөні)/(фамилия, инициалы)

20___ жылғы _____
№___ ағымдағы банктік шот шартына
№___ қосымша келісімге
№6 қосымша

(заңды тұлғалар, жеке кәсіпкерлер, шаруа немесе фермер қожалықтары, жеке нотариустер (жалпы шаруашылық мақсаттар), жеке сот орындаушылар (жалпы шаруашылық мақсаттар) және адвокаттар үшін)

Приложение №-6
К Дополнительному соглашению №__
к Договору текущего банковского счета №_____ от _____ 20___ года

(для юридических лиц, индивидуальных предпринимателей, крестьянских или фермерских хозяйств, частных нотариусов (общехозяйственные цели), частных судебных исполнителей (общехозяйственные цели) и адвокатов)
к Дополнительному

ҚБҚ-та орнату актісі/
Акт установки в ДБО

г._____қ. 20___ж./г. «____»_____

Осы Акт /Настоящий Акт свидетельствует о том, что _____ 20__ ж./г. «___» _____ № _____ өтінімінің толық орындалғанын куәландырады. /Заявка выполнена в полном объёме.
_____
_____
(кілт иесінің лауазымы және тегі, аты, әкесінің аты) / (должность и фамилия, имя, отчество владельца ключа)

келесі әрекеттер жүзеге асырылды/ были осуществлены следующие действия:
- ☐ Браузер және active X күйге келтіру/ Настройка браузера и active X
- ☐ ҚБҚ-да жұмыс істеуге үйрету/ Обучение в работе ДБО

«Еуразиялық банк» АҚ-та «Client's Bank» заңды тұлғаларға қашықтықтан банктік қызмет көрсету жүйесі / Системы дистанционного банковского обслуживания юридических лиц «Client's Bank» в АО «Евразийский банк».

Сонымен қатар келесі тесттік операциялар жүргізілді/ Также были совершены следующие тестовые операции:

1) барлық шоттар бойынша өткен күн үшін үзінді-көшірме мен ағымдағы күн үшін анықтама құрастыру / формирование выписки за предыдущий день и справки за текущий по всем счетам;
2) төлем тапсырмасын теңгеде ресімдеу / оформление платёжного поручения в тенге;
3) тізімдермен бірге импортталатын зейнетақы және әлеуметтік төлемдерді жүргізу (MT102 пішімінде немесе меншікті 1С форматында) / проведение импортированных пенсионного и социального платежей со списками (в формате MT102 или в собственном формате 1С);
4) шетел валютасында аударым жасауға өтініш (шетел валютасында шот болған жағдайда) ресімдеу/ оформление заявления на перевод в иностранной валюте (в случае если имеется счет в иностранной валюте);
5) шетел валютасын айырбастауға өтініш жүргізу (шетел валютасында шот болған жағдайда) / проведение заявления на конвертацию иностранной валюты (в случае если имеется счет в иностранной валюте);
6) Банкке қосымшасымен бірге хат жолдау / отправка письма в Банк с приложением;
7) валюталар бағамы қарастырылады / просматриваются курсы валют;
8) кредиттік/депозиттік/карточкалық шоттарды қарастыру/просмотр кредитных/депозитных/карточных счетов;
9) клиенттің АЖО бухгалтерлік бағдарламаға үзінді-көшірмелер экспорттау (1С қолданылған жағдайда) / экспорт выписки из АРМ клиента в бухгалтерскую программу (в случае использования 1С);

Орындалған жұмыстар бойынша Тараптардың бір-біріне наразылықтары жоқ / Претензий по выполненной работе Стороны друг к другу не имеют.

Күні/Дата: ____/_____/_____ Уақыты/Время: _____/_____

күн/день ай/месяц жыл/год **сағат/часы минут/минуты**

Инженердің қолы/ Подпись Инженера **Клиенттің қолы/ Подпись Клиента**

_____/_____ _____/_____
қолы/ подпись ТАӘ/ ФИО қолы/ подпись ТАӘ/ ФИО

МО/ МП