Қосылу шартына № 9 қосымша/Приложение № 9 к Договору присоединения

ҚБҚК Пайдаланушыларын қосуға /өзгертуге /алып тастауға
№8 өтініш-оферта (қажеттісін таңдап, толтыру)
/ Заявление-оферта №8
на подключение /изменение /отключение Пользователей ДБО[1] /(необходимое выбрать и заполнить)

г._____ қ.

Клиенттің толық атауы /Полное наименование Клиента
_____
орналасқан мекенжайы: /расположенного по адресу _____
Филиалда (негізгі) қызмет көрсетіледі/обслуживающийся в Филиале (основной)_____

☐ **Жаңа ҚБҚК пайдаланушысын қосу/Подключить нового пользователя ДБО**

ТАӘ /ФИО	**Жеке басын куәландыратын құжаттың нөмірі /Номер документа, удостоверяющий личность**	**Электрондық мекенжайы /Электронный адрес**	**Ұялы телефон нөмірі /Номер мобильного телефона**	**Қол қою құқығы /Право подписи**	**ОТР құрылғысының сериялық нөмірі (қолдану кезінде) /Серийный номер ОТР устройства (при использовании)**
			+7(_ _ _)_ _ _ _ _ _ _		
			+7(_ _ _)_ _ _ _ _ _ _		
			+7(_ _ _)_ _ _ _ _ _ _		
			+7(_ _ _)_ _ _ _ _ _ _		
			+7(_ _ _)_ _ _ _ _ _ _		

[1] ҚБҚК-қашықтан банктік қызмет көрсету/ДБО – дистанционное банковское обслуживание

☐ **ҚБҚК пайдаланушыны «Кеңейтілген құқықтар» қызметіне қосымша қосу (қажет болған жағдайда)/Дополнительно подключить пользователя ДБО к услуге «Расширенные права» (при необходимости)**

ТАӘ /ФИО	Қол қою құқығы /Право подписи	Шот/Барлық шоттар /Счет/Все счета	Құжаттың ең көп сомасы (соманы көрсету)/Максимальная сумма документа (указать сумму)

☐ **Бұрын қосылған пайдаланушыға өзгерістер енгізу (қажеттісін толтыру)/Внести изменения к ранее подключенному пользователю (нужное заполнить)**

ТАӘ /ФИО	Электрондық мекенжайы /Электронный адрес	Ұялы телефон нөмірі /Номер мобильного телефона	Қол қою құқығы /Право подписи	OTP құрылғысының сериялық нөмірі /Серийный номер OTP устройства
		+7(_ _ _)_ _ _ _ _ _ _		
		+7(_ _ _)_ _ _ _ _ _ _		
		+7(_ _ _)_ _ _ _ _ _ _		

☐ **ҚБҚК пайдаланушысын алып тастау/оқшаулау. OTP құрылғыны ағыту (бар болса)/Отключить/блокировать пользователя ДБО. Отвязать OTP устройства (при наличии)**

ТАӘ /ФИО	Себебі /Причина	Қол қою құқығы /Право подписи	№ OTP

ҚБҚК-ғы Клиенттің Жұмыс орнының ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі талаптар мен ұсыныстар

1. Жалпы ережелер

1.1. «ҚБҚК WEB-интерфейсінің ақпараттық қауіпсіздігі кешендік (ұйымдық, әкімшілік, техникалық және бағдарламалық) шаралармен және құралдармен қамтамасыз етілуі тиіс.

1.2. Ақпарат қауіпсіздігін қамтамасыз ету мақсатында:

- Клиенттің басшылығы әрбір пайдаланушыға нақты функциялар мен өкілеттіктерді бекітіп берумен ҚБҚК-дағы жұмысқа рұқсаты бар пайдаланушылар мен әкімшілердің тізімін бекітуі тиіс;
- Клиенттің басшылығы ҚБҚК қауіпсіздігін қамтамасыз етуге жауапты қызметкер тағайындауы тиіс;
- ҚБҚК пайдаланушылар ҚБҚ құжаттамасы мен осы әдістемелік нұсқаулықтарға сәйкес пайдалану ережелерімен таныстырылуы тиіс;
- ҚБҚК-ға кіру деректері мен ОТР құрылғылары рұқсатсыз кіруден (РК) қорғалуы керек.

1.3. Өз компьютерінде қауіпсіз ортаны қамтамасыз ету үшін Клиент:

- Электронды хаттарды сүзгілеу үшін .exe .cmd .bat .dll ықтимал қауіпті қосымшаларды оқшаулайтын БЖ орнатуы тиіс;
- Туындайтын қателіктерді, пайдаланушылардың кіруін және бағдарламалардың іске қосылуын тіркейтін жүйелік оқиғалар аудитін іске қосып, кезеңді түрде журналды тексеріп, қателіктерге назар аударып отыруы тиіс;
- Компьютердің вируспен зақымданғаны жөнінде күдік туындаған жағдайда жұмыс станцияларын тексеруі тиіс.

2. ҚБҚК-ны рұқсатсыз кіруден (РК) қорғау жөніндегі талаптар

2.1. ҚБҚК-ға және ОТР құрылғыларына кіру деректерін рұқсатсыз кіруден қорғау келесі мүмкіндіктерді жою мақсатында жүзеге асырылады:

- ҚБҚК-мен жұмыс істейтін компьютерлерде компьютерлік вирустар мен ҚБҚК БЖ бүлдіруге, жұмыс қабілеттілігін бұзуға немесе түрлендіруге немесе ақпаратты қолға түсіруге бағытталған бағдарламалардың пайда болуы;
- ҚБҚК техникалық және бағдарламалық құралдарына, сондай-ақ олардың құрамына рұқсатсыз өзгерістердің енгізілуі;
- Электрондық құжатқа (ЭҚ) рұқсатсыз өзгерістердің енгізілуі.

2.2. ҚБҚК-ны жеке бөлінген дербес компьютерде пайдалану ұсынылады. Бұл компьютер міндетті түрде желілік шабуылдардан қорғаныспен және вирусқа қарсы қорғаныспен қамтамасыз етілуі тиіс.

2.3. ҚБҚК-ны рұқсатсыз кіруден қорғау мақсатында компьютерлерге рұқсатсыз кіруден қорғаудың бағдарламалық-аппараттық кешенін орнату ұсынылады.

2.4. РК-дан қорғаныс кешенінің көмегімен ҚБҚК тұтастығын бақылауды қамтамасыз ететін және пайдаланушылардың жұмысын оларға берілетін мүмкіндіктер мен өкілеттіктер аясында ғана жасауға мүмкіндік беретін функционалды тұйық ортаны қалыптастыру ұсынылады.

2.5. ҚБҚК-мен жұмыс үшін пайдаланылатын дербес компьютерде БЖ әзірлеу құралдары мен оңдауыштар орнатылмауы тиіс.

2.6. Компьютерлерді РК-дан қорғау үшін сондай-ақ операциялық жүйенің штаттық мүмкіндіктері пайдаланылуы тиіс.

3. ОТР құрылғыларын сақтауды және пайдалануды ұйымдастыру жөніндегі талаптар

3.1. ОТР құрылғылары тек олар тиесілі тұлғаларда ғана сақталуы тиіс.

3.2. ОТР құрылғыларына қолжетімділігі бар тұлғалардың тізімі бекітіп берілген функциялары мен өкілеттіктеріне сәйкес Клиент басшылығының бұйрығымен немесе өкімімен анықталады.

3.3. ОТР құрылғыларымен жұмыс жасау кезінде бөтен тұлғалардың оларға қол жеткізуін болдырмау қажет.

3.4. ОТР құрылғыларын сақтау үшін сенімді металл сейфтері орнатылуы тиіс.

3.5. Жұмыс күні аяқталғанда, сондай-ақ Банкпен байланыс жасау сеанстарынан тыс уақытта ОТР құрылғылары сейфте сақталуы тиіс.

3.6. ОТР құрылғыларын басқа құжаттармен олардан бөлек және бөтен тұлғалардың оларға жасырын қол жеткізу мүмкіндігін болдырмайтындай орамада бір сейфте сақтауға рұқсат беріледі.

3.7. Келесілерге рұқсат берілмейді:

- ОТР құрылғыларын олармен жұмыс жасауға рұқсаты жоқ тұлғаларға беру:

- құпия кілттерді дисплейге немесе принтерден шығару;
- ОТР құрылғыларын жұмыс орнында қараусыз қалдыру;

4. ҚБҚК-ны рұқсатсыз кіруден қорғау жөніндегі практикалық ұсыныстар

4.1. ҚБҚК-ға желілік қолжетімділікті (оның ішінде желіге қашықтан кіруді) жергілікті желінің басқа жұмыс станцияларынан және әсіресе сыртқы желілерден толығымен оқшаулау ұсынылады.

4.2. ҚБҚК пайдаланушыларын Интернет желісін пайдаланудан шектеу ұсынылады. Міндетті түрде вирусқа қарсы бағдарламалық жасақтаманы орнатып және оны ұдайы жаңартып отыру қажет.

4.3. Осы есептік жазбалар бойынша компьютерде бағдарламалық жасақтаманы орнату мүмкіндігін шектеу мақсатында жүйемен жұмыс жасайтын ҚБҚК пайдаланушыларына әкімші құқығы берілмеуі тиіс. Компьютердің файлдық ресурстарына, әсіресе жазбаға қол жеткізу минималды қажетті құқықтармен шектелуі тиіс. Пайдаланушылар тек қана оларға рұқсат етілген қосымшаларды ғана іске қосуы тиіс.

4.4. ҚБҚК пайдаланушылары міндетті түрде негізгі қауіпсіздік талаптарын сақтау мәселелері бойынша, әсіресе вирусқа қарсы бағдарламаларды пайдалану мәселелері бойынша нұсқаулықтар алуы тиіс.

4.5. Жергілікті (немесе домендік) саясаттармен компьютерде операциялық жүйеге кіру мүмкіндігі бар пайдаланушылардың тізімін шектеу ұсынылады.

4.6. Сыртқы электрондық поштаны (Интернет желісінен) қабылдауды шектеу немесе толығымен бас тарту ұсынылады. Алынатын пошта міндетті түрде вирусқа қарсы құралдармен тексерілуі тиіс.

4.7. Компьютерде тек бір ғана ОЖ орнатылуы тиіс.

4.8. Операциялық жүйенің пайдаланушыларына құпиясөздер тағайындалуы тиіс. Құпиясөз ұзындығы кемінде алты таңбадан тұруы керек. Құпиясөздің қолданылу мерзімі шектелуі тиіс.

4.9. Рұқсатсыз ашуды болдырмау үшін компьютердің жүйелік блогына сүргі салу ұсынылады.

4.10. Компьютерге қолжетімділікті шектеу, пайдаланылатын БЖ тұтастығын тексеру үшін компьютерге РК-дан қорғаудың бағдарламалық-аппараттық кешенін («Аккорд», «Соболь» және т.с.с.) орнатып, оны баптау ұсынылады.

4.11. Компьютерге сыртқы құрылғыларды, оның ішінде өндірістік қажеттілікпен қарастырылмаған ақпарат тасымалдағыштарды қосуға болмайды.

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

1. Общие положения

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

1.2. 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 работник 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 ОТР устройства должны быть защищены от несанкционированного доступа (НСД).

1.4. Для обеспечения безопасной среды на своем компьютере Клиенту надлежит:

- Установить ПО 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.

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

2.1. Защита данных для входа в ДБО и ОТР устройств от несанкционированного доступа осуществляется с целью исключения возможностей:

- появления в компьютерах, на которых работают в системе 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 ДБО, а также в их состав;
- внесения несанкционированных изменений в Электронный документ (ЭД).

2.2. ДБО рекомендуется использовать на отдельном выделенном персональном компьютере. Должна быть обеспечена в обязательном порядке защита данного компьютера от сетевых атак и антивирусная защита.

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

2.4. 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.

2.5. На персональном компьютере, используемом для работы с ДБО не должны устанавливаться средства разработки ПО и отладчики.

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

3. Требования по организации хранения и использования ОТР устройств

3.1. ОТР устройства должны храниться только у тех лиц, которым они принадлежат.

3.2. Список лиц, имеющих доступ к ОТР устройствам, определяется приказом или распоряжением руководства Клиента, согласно закрепленными за ними функциями и полномочиями.

3.3. Во время работы с ОТР устройствами доступ к ним посторонних лиц должен быть исключен.

3.4. Для хранения ОТР устройств должны устанавливаться надежные металлические сейфы.

3.5. По окончании рабочего дня, а также вне времени сеансов связи с Банком ОТР устройства должны храниться в сейфе.

3.6. Хранение ОТР устройств допускается в одном сейфе с другими документами, отдельно от них и в упаковке, исключающей возможность негласного доступа к ним посторонних лиц.

3.7. Не разрешается:

- передавать ОТР устройства лицам, к ним не допущенным;
- выводить секретные ключи на дисплей или принтер;
- оставлять ОТР устройства без присмотра на рабочем месте;

4. Практические рекомендации по защите ДБО от несанкционированного доступа

4.1. 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.

4.2. Рекомендуется ограничить использование сети Интернет-пользователями ДБО. В обязательном порядке должно быть установлено и регулярно обновляться антивирусное программное обеспечение.

4.3. 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.

4.4. Пользователи ДБО, должны быть в обязательном порядке проинструктированы по вопросам соблюдения основных требований безопасности, и в особенности по вопросам использования антивирусных программ.

4.5. Локальными (или доменными) политиками на компьютере рекомендуется ограничить список пользователей, имеющих возможность входа в операционную систему.
4.6. Рекомендуется ограничить или полностью отказаться от приема внешней (из Сети Интернет) электронной почты. В обязательном порядке получаемая почта должна проверяться антивирусными средствами.
4.7. На компьютере должна быть установлена только одна ОС.
4.8. Пользователям операционной системы должны быть назначены пароли. Длина паролей должна составлять не менее шести символов. Срок действия паролей должен быть ограничен.
4.9. Рекомендуется опечатать системный блок компьютера для предотвращения его несанкционированного вскрытия.
4.10. 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.).
4.11. Не рекомендуется подключать к компьютеру внешние устройства, в том числе носители информации, не предусмотренные производственной необходимостью.

«Клиент»:
Т.А.Ә. /Ф.И.О _____
Лауазымы /Должность _____
Қолы /Подпись _____
М.О (бар болса)/М.П. (при наличии)
Күні /Дата____/_____/_____ Уақыты /Время_____ сағ /ч/_____мин

Банктің белгілері/Отметки Банка:
Өтінішті қабылдаған /Заявление принял _____ _____
Қолы/Подпись *Т.А.Ә./Ф.И.О.* М.О. (мөр болса) /М.П. (при наличии)
Фронт-офис бөлімшесінің жетекшісі:/Руководитель подразделения фронт-офиса: _____

20___ жылғы «___» _____
/«____» _____20__ г.