Приложение № 5

к Договору долгосрочной аренды

нежилого помещения № от « » 20 г.

Положение о соблюдении требований кибербезопасности ПАО Сбербанк

Реализуя принятые ПАО Сбербанк (далее по тексту – Банк, Арендатор) политики о соблюдении требований кибербезопасности,  (далее – Контрагент, Арендодатель) гарантирует соблюдение в рамках исполнения заключенного договора с Банком (далее – Договор), в том числе при установлении, изменении, расторжении договорных отношений, следующих положений:

1.1. Контрагент обязан соблюдать требования законодательства РФ, требования регулирующих органов (ФСБ, ФСТЭК, ЦБ, Минкомсвязь) в области защиты информации и обладать необходимыми лицензиями и сертификатами для исполнения принятых на себя обязательств по Договору.

1.2. Стороны согласовали следующие условия:

• до начала исполнения условий Договора Контрагент обязан заключить Соглашение о неразглашении конфиденциальной информации;

• подключение любого оборудования к ИТ-инфраструктуре Банка допускается только в целях исполнения обязательств по Договору в соответствии с установленными нормативными документами Банка. Контрагент обязан согласовать данное подключение с ответственными лицами со стороны Банка (пункт 1.10 настоящего Положения). Требования к подключаемому оборудованию должны соответствовать нормативным документам Банка;

• при подключении ИТ-инфраструктуры Контрагента к ИТ-инфраструктуре Банка Стороны заключают Соглашение о кибербезопасности. При этом Контрагент обязан заблаговременно осуществить все необходимые мероприятия, обеспечивающие возможность надлежащего применения Соглашения о кибербезопасности.

• допуск работников Контрагента к автоматизированным системам, оборудованию, средствам вычислительной техники (далее – СВТ) и в помещения Банка производится после подписания работниками Контрагента «Обязательства о соблюдении требований кибербезопасности в ПАО Сбербанк» (Приложение №1 к настоящему Положению). При этом, доступ к СВТ Банка, содержащим сведения, имеющие отношение к банковской тайне, в рамках Договора не предоставляется. Контрагент обязуется по требованию Банка предоставить подписанное работником Контрагента Обязательство о соблюдении требований кибербезопасности ПАО Сбербанк в течение 3 (трех) рабочих дней с даты получения соответствующего требования.

В случае нарушения Контрагентом настоящих условий, требований Соглашения о кибербезопасности, Обязательства о соблюдении требований кибербезопасности в ПАО Сбербанк, Банк вправе отказаться от Договора в любое время без возмещения убытков Контрагенту, путём направления Контрагенту соответствующего уведомления не менее чем за 5 (пять) рабочих дней до момента прекращения Договора. Банк вправе отказать Контрагенту в предоставлении доступа к своей ИТ-инфраструктуре.

1.3. Контрагент гарантирует, что исполнение условий Договора не приведет к появлению скрытых функциональных возможностей (недокументированных изменений, операций либо внедренных «программных закладок»), а также компьютерных вирусов, троянов, самоликвидирующихся механизмов, механизмов защиты от копирования и других подобных машинных команд, которые могут деактивировать, уничтожить или изменить иным образом данные Банка, программное или аппаратное обеспечение и оборудование Банка.

1.4. Контрагент гарантирует, что исполнение условий Договора не приведет к появлению в программном обеспечении Банка без предварительного письменного согласования со стороны Банка, программного обеспечения, используемого на условиях открытых лицензий (free and open-source software). И, безусловно, не приведет к появлению в программном обеспечении Банка, программного обеспечения, используемого на основании открытых лицензий, условия которых требуют от пользователя раскрытия исходного кода модифицированного ПО, либо ограничивают право пользователя запрещать третьим лицам использование модифицированного ПО. Под программным обеспечением Банка в рамках настоящего Положения понимается программное обеспечение, исключительное право на которое принадлежит Банку на момент заключения Договора и/или возникает (переходит) у Банка в результате надлежащего исполнения Договора.

1.5. При выполнении работ/ оказании услуг по техническому обслуживанию и поддержке, Контрагент несет ответственность за своевременное обновление системного и прикладного ПО оборудования и СВТ Банка, не подключенных к ИТ-инфраструктуре Банка.

1.6. В каждом случае нарушений гарантий, указанных в п. п. 1.3.-1.4., Контрагент выплачивает Банку штрафную неустойку в размере 0,1 (Ноль целых одна десятая) % от общего размера вознаграждения, указанного в Договоре, но не более 10 (Десяти) %. Также Контрагент обязуется в полном объёме возместить убытки, причинённые Банку вследствие нарушения Контрагентом гарантий, указанных в п.п. 1.3.-1.4. Взыскание убытков не лишает Банк возможности прибегать к любым иным мерам защиты своих прав и интересов, предусмотренных действующим законодательством и соглашением Сторон, в том числе взысканию неустойки в полном размере сверх убытков.

1.7. Контрагент обязуется передавать поставляемое, разрабатываемое, дорабатываемое (модифицируемое, адаптируемое) в интересах Банка ПО перед сдачей-приемкой работ по договору Банку для тестирования и приемки с участием специалистов Банка, в соответствии с установленными у Банка внутренними процедурами. При отрицательном результате прохождения тестирования или приемки ввод ПО в эксплуатацию запрещен, работа считается невыполненной и акт приема-сдачи работ не подписывается. В целях проведения тестирования и приемки эталонный дистрибутив и исходные коды ПО (в случае передачи исходных кодов ПО в соответствии с условиями соглашения между Сторонами) передается на хранение в фонд программ и документации (ФПД) Банка до проведения приемки. Для целей проведения тестирования и приемки между Сторонами заключается лицензионное соглашение, по которому Контрагент предоставляет Банку на безвозмездной основе (без выплаты лицензионного вознаграждения) право использования такого ПО всеми способами и на условиях, необходимых для проведения тестирования и приемки .

1.8. В случае если Банк сочтет необходимым, с исходных кодов на оборудовании Банка в присутствии Контрагента проводится контрольная компиляция ПО, в соответствии с установленными у Банка внутренними процедурами. В случае если исходные коды ПО не передаются, после проведения контрольной компиляции осуществляется удаление исходных кодов ПО с оборудования Банка.

Для высококритичных систем может применяться процедура депонирования исходных кодов, регулируемая отдельным соглашением Банка и Контрагента.

1.9. Контрагент в рамках исполнения обязательств по Договору вправе привлекать субподрядчиков с соблюдением следующих условий:

• привлечение субподрядчика Контрагент обязан предварительно письменно согласовать с Банком;

• субподрядчик соблюдает все требования настоящего Положения;

• запрещено самостоятельное подключение Контрагентом субподрядчика к ИТ-инфраструктуре Банка и/или предоставление доступа к СВТ и АС Банка без письменного согласования ответственного за взаимодействие по вопросам КБ и ИТ со стороны Банка и выполнения субподрядчиком условий, определенных Банком;

• в случае необходимости передачи субподрядчику защищаемой информации порядок такой передачи, условия передачи и обработки, требования к защите информации определяются отдельным договором между Банком и субподрядчиком.

1.10. Стороны назначают ответственных лиц за взаимодействие и организацию контроля по Договору в части:

• Организации и взаимодействие по вопросам ИТ, связанных с исполнением предмета Договора:

|  |  |
| --- | --- |
| **От Банка:**  ФИО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Должность: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Подразделение: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Контакты (тел/почта): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **От Контрагента:**  ФИО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Должность: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Подразделение: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Контакты (тел/почта): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

• Организации взаимодействия по КБ:

|  |  |
| --- | --- |
| **От Банка:**  Подразделение: Центр внутрикорпоративного взаимодействия  Контакты: +7 495 66 55 600 или +7 495 669 0 999 доб. 69 500  cyber\_acord@sberbank.ru | **От Контрагента:**  ФИО: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Должность: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Подразделение: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Контакты (тел/почта): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

1.11. Контрагент обязан информировать Банк обо всех фактах нарушения требований настоящего Положения или событиях, способных привести к таким нарушениям. Информирование осуществляется в максимально короткий срок, но не позднее 24 часов с момента обнаружения факта через Ответственного за организацию контроля и взаимодействие соблюдения требовании КБ со стороны Банка, а в случае экстренной ситуации – по телефону +7 (495) 967-3980, доб.33379, и/или e-mail: ZIT@sberbank.ru.

1.12. Контрагент несет ответственность:

• за соблюдение требований настоящего Положения;

• за действия своих работников, выполняющих работы в помещениях и на СВТ Банка;

• за все действия привлекаемых ими субподрядчиков.

1.13. В случае нарушения требований настоящего Положения, повлекшего возникновение значимого инцидента КБ в ИТ инфраструктуре Банка, а также являющегося следствием инцидента, возникшего на стороне Контрагента, Контрагент обязан выплатить Банку штраф в размере 10 (десяти) % от стоимости Договора за каждый инцидент, а также полностью возместить Банку причиненные ему убытки.

|  |  |
| --- | --- |
| **От Арендатора:**  Заместитель управляющего  Омским отделением № 8634  ПАО Сбербанк  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Мусалимова С.С. /  м. п. | **От Арендодателя:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / /  м. п. |

Приложение №1

к Положению о соблюдении

требований кибербезопасности ПАО Сбербанк

ОБЯЗАТЕЛЬСТВО

о соблюдении требований кибербезопасности в ПАО Сбербанк

Я,  являясь , (далее - Контрагент), обязуюсь выполнять перечисленные ниже требования:

1. Использовать предоставленный мне доступ к автоматизированным системам (АС) Банка, оборудованию, средствам вычислительной техники (СВТ) и помещениям исключительно в целях исполнения обязательств по заключенным с Банком договорам (далее – Работы/Услуги).

2. Не разглашать и не использовать в личных целях и целях третьих лиц конфиденциальную информацию, доступ к которой предоставлен мне для проведения Работ, соблюдать требования режима коммерческой тайны Банка.

3. Не обсуждать на форумах и в конференциях сети Интернет вопросы, касающиеся моей профессиональной деятельности в части отношений с Банком и его работниками.

4. Препятствовать ознакомлению посторонних лиц с конфиденциальными документами, не допускать утрату (кражу, порчу, утерю) материальных носителей (USB-носителей, оптических дисков, внешних жестких дисков и др.), содержащих конфиденциальную информацию Банка.

5. Не хранить конфиденциальную информацию Банка в общедоступных ресурсах, не передавать ее за пределы сетей Банка в открытом (незащищенном от доступа посторонних лиц) виде, не использовать для передачи конфиденциальной информации общедоступные интернет-мессенджеры (Viber, WhatsApp, Telegram, Skype и т.д.).

6. Без лишней необходимости не распечатывать электронные конфиденциальные документы, забирать свои распечатанные документы из принтеров сразу после окончания печати и удалять файлы из папок сканирования.

7. По завершению использования, уничтожать документы и медиа-носители, содержащие конфиденциальную информацию, методом механической переработки с помощью уничтожителей бумаг (шредеров).

8. При работе с СВТ Банка:

8.1. Оставляя рабочее место, блокировать его (комбинацией Win+L для систем под управлением Windows или Command+Control+Q для систем с Mac OS).

8.2. Не прерывать сканирование антивирусным ПО съемных машинных и медиа носителей информации (USB-носителей, оптических дисков, внешних жестких дисков и др.) при их подключении к автоматизированному рабочему месту (АРМ), включенному в сеть Банка.

8.3. Соблюдать парольную политику в части удовлетворения следующим требованиям

• длина пароля должна быть не менее 8 символов;

• пароль должен содержать в себе символы как минимум трех категорий из четырех: буквы нижнего регистра (от a до z), буквы верхнего регистра (от A до Z), цифры (от 0 до 9) и спецсимволы (например: $, #, %);

• пароль не должен совпадать с логином и повторять предыдущие 4 пароля для данной учетной записи пользователя;

• пароль не должен включать осмысленные слова, словосочетания, общепринятые аббревиатуры, а также основываться на доступных данных о пользователе (фамилии, дате рождения, именах родственников, номеров телефонов и др.) или легко угадываемом алгоритме смены (Smi1le!, Smi2le!, Smi3le! и т.д.);

• пароль не должен содержать широко известные или легко угадываемые слова и последовательности символов (12345678, password, qwerty, aaabbb и т.д.)

• пароль по умолчанию (созданный при создании учетной записи пользователя) должен быть изменен пользователем при первом входе;

• пароль должен изменяться не реже чем 1 раз в 40 дней с момента последнего изменения;

• в случае разглашения или компрометации пароль должен быть незамедлительно изменен.

8.4. Соблюдать правила обращения с паролями:

• не записывать пароль на предметах и материальных носителях, а также не хранить его в файле в открытом виде;

• не использовать один и тот же пароль для различных учетных записей;

• не передавать кому-либо (в т.ч. своим коллегам и руководителям, а также работникам Банка) свой пароль, равно как и использовать чужие пароли для работы с СВТ и АС Банка;

• не осуществлять попытки подбора паролей (в том числе автоматизированными способами), не пытаться завладеть паролями других лиц.

8.5. Не организовывать на предоставленном компьютере ресурсы общего доступа и сетевые сервисы (открывать доступ к общим папкам, дискам, CD-приводам и дисководам, настраивать службы удаленного доступа, прокси- или веб-серверы, беспроводные точки доступа, Bluetooth интерфейсы и т.д.).

8.6. Не предпринимать попытки преодоления установленных Банком ограничений, отключать и/или удалять установленные на предоставленных СВТ Банка средства защиты информации (в том числе антивирусное программное обеспечение), использовать недокументированные свойства, ошибки в программном обеспечении (ПО) и настройках защиты доступа к информационным ресурсам и АС Банка, доступ к которым не был предоставлен явным образом.

8.7. Не устанавливать на предоставленные СВТ какое-либо программное обеспечение кроме ПО принятого в ФПД Банка, изменять настройки уже имеющегося. По вопросам установки необходимого ПО, а также получения административных прав в операционных системах персональных компьютеров обращаться к ответственному лицу Контрагента (для дочерних и зависимых обществ Банка) или Банка, назначенному в соответствии с пунктом 1.10 Положения о соблюдении требований кибербезопасности ПАО Сбербанк.

8.8. Не хранить и не использовать на предоставленном компьютере программное обеспечение, фонограммы и другие результаты интеллектуальной деятельности в нарушение прав их законных правообладателей.

8.9. Не открывать вложения и не переходить по ссылкам, указанным в почтовых сообщениях, имеющих признаки фишинга, включая:

• сообщение замаскировано под официальное письмо организации и требует каких-либо быстрых действий или ответа;

• сообщение содержит ссылки на интернет-ресурсы, визуально похожие на оригинальные ресурсы организации, однако в отношении которых возникают сомнения;

• к сообщению прикреплен файл-вложение, который настойчиво предлагается открыть;

• в тексте сообщения содержатся опечатки, ошибки, избыточные знаки препинания;

8.10. не переходить по коротким ссылкам вида bit.ly или goo.gl.

8.11. не вскрывать корпус предоставленного компьютера (в том числе для самостоятельного устранения неисправностей), самовольно подключать к нему какое-либо оборудование (GPRS модемы, Wi-Fi точки доступа и пр.).

8.12. не подключать к предоставленным СВТ Банка личные мобильные устройства (телефоны, смартфоны, планшетные компьютеры, ноутбуки), беспроводные (радио) интерфейсы, модемы и прочее оборудование, позволяющее выходить в сеть Интернет и другие публичные сети.

9. Не использовать ПО следующих категорий при подключении к корпоративной сети Банка :

• сканеры портов и анализаторы трафика;

• средства для организации удаленного доступа, не утвержденные требованиями Банка;

• ПО, используемое для анонимного доступа в сеть Интернет (включая веб-сервисы, прокси-серверы) и/или создания зашифрованных каналов связи (VPN-, DNS-, SSH-, HTTPS-туннели и пр.);

• ПО для обхода средств защиты, включая средства подбора и восстановления паролей, поиска уязвимостей;

• ПО, предназначенное для сокрытия или внедрения дополнительной информации в цифровые объекты (в том числе реализующее методы стеганографии);

• ПО, осуществляющее сбор информации с клавиатуры, экрана, микрофона (снифферы);

• специализированные программные средства, оказывающее влияние на сетевые настройки СВТ, серверов и сетевого оборудования;

• средства виртуализации.

10. Не рассылать из корпоративной сети и корпоративных почтовых адресов Банка сообщений развлекательного, рекламного и иного характера, не относящегося к проведению Работ.

11. Не использовать АРМ Банка (в том числе с использованием расширений к web-браузеру) и личные СВТ, подключенные к сетям Банка, для посещения интернет-ресурсов:

• содержание и направленность которых запрещены международным и российским законодательством;

• содержащих материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц;

• содержащих материалы, способствующие разжиганию межнациональной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия и т.д.

12. Не оставлять без присмотра или передавать кому-либо предоставленные ТМ-идентификаторы, пропуска и прочие средства идентификации, а также ключи от помещений Банка.

13. По требованию уполномоченных представителей Банка предоставлять выданные СВТ и носители информации (USB-Flash, CD/DVD и др.) для проверки выполнения требований информационной безопасности.

14. Информировать ответственное лицо Банка по вопросам кибербезопасности обо всех инцидентах КБ и событий, создающих угрозу причинения ущерба Банку, а также об обращениях третьих лиц с целью незаконного получения конфиденциальной информации Банка.

Я предупрежден(а) о том, что, Банк вправе контролировать мои действия при работе с АС Банка, оборудованием и средствами вычислительной техники, включая анализ отправленных мной информационных сообщений, в т.ч. с использованием корпоративных почтовых систем Банка и с использованием сети Интернет.

Я предупрежден(а) о том, что Банк вправе использовать полученную в результате такого анализа информацию для проведения расследований, в том числе, с привлечением правоохранительных органов, а также использовать в качестве доказательств в суде, и подтверждаю, что в этих случаях я не вправе рассчитывать на соблюдение в отношении этих сообщений конфиденциальности со стороны Банка.

Я понимаю, что в случае выявления нарушений перечисленных требований, повлекших причинение ущерба Банку, Банк вправе отстранить меня от Работ, приостановить мой доступ к своим АС, оборудованию СВТ и в помещения, а в случае подтверждения факта ущерба, требовать его возмещения от Контрагента, в т.ч. в судебном порядке.

С выпиской из УК РФ (ст.146, 183, 272, 273 и 274) ознакомлен (а). С перечнем информации, составляющей коммерческую тайну, и режимом коммерческой тайны ПАО Сбербанк ознакомлен(а) и обязуюсь исполнять.

Настоящее Обязательство составлено в 3 (трех) экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для Банка и Колмогорова Дмитрия Викторовича и 1 (один) экземпляр для органа, осуществляющего государственную регистрацию прав на недвижимое имущество и сделок с ним.

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_г.              \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Подпись                          ФИО*

**Подписи сторон:**

|  |  |
| --- | --- |
| **От Арендатора:**  Заместитель управляющего  Омским отделением № 8634  ПАО Сбербанк  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/ Мусалимова С.С. /  м. п. | **От Арендодателя:**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / /  м. п. |