

Требования

о предоставлении оборудования для целей исполнения обязанностей по Договору (далее – «Требования»)

1. Общие положения.

1.1. Предприятие обязуется предоставить Контрагенту оборудование Предприятия, в том числе персональные компьютеры, а Контрагент обязуется пользоваться оборудованием на условиях, предусмотренных настоящими требованиями. Оборудование передается Контрагенту по акту приема-передачи. Форма указанного акта предусмотрена Приложением №1 к настоящим Требованиям.

1.2. Предприятие предоставляет Контрагенту оборудование только для целей исполнения обязанностей Контрагента в рамках договора между Предприятием и Контрагентом, в котором содержится ссылка на настоящие Требования (далее – «Договор»). Контрагент обязуется использовать оборудование исключительно в интересах Предприятия.

1.3. Оборудование предоставляется Контрагенту на время исполнения Договора. Персональные компьютеры, предоставляемые Контрагенту, должны иметь:

- подключение к МФУ, принтерам, копирам, сканерам, факсам коллективного доступа, которые установлены в копировальных центрах/комнатах печати Предприятия;

- подключение к домену Предприятия с уровнем доступа, минимально необходимым для исполнения Договора, при этом Контрагенту не передаются пароли, права, полномочия и привилегии на системное администрирование серверов, администрирование активного сетевого оборудования, администрирование систем управления базами данных, администрирование бизнес приложений (находящихся в эксплуатации), права администратора на рабочие станции. В случае попадания указанных паролей доступа, прав, полномочий и привилегий (умышленного или случайного) третьим лицам Контрагент не вправе их использовать и обязан незамедлительно сообщить об этом Предприятию, и предпринять действия по устранению указанной проблемы.

1.4. Оборудование, предоставленное Контрагенту, должно использоваться только работниками Контрагента, предоставление Контрагентом третьим лицам доступа к пользованию указанным оборудованием не допускается. Под работниками Контрагента понимаются физические лица, привлеченные Контрагентом по трудовым или гражданско-правовым договорам.

Контрагент подтверждает, что он ознакомлен со всеми внутренними процедурами, локальными актами Предприятия, регламентирующими порядок использования оборудования, предоставленного Контрагенту, и устанавливающими требования в области информационной безопасности. Контрагент обязуется до начала исполнения обязательств по Договору ознакомить с указанными процедурами, локальными актами всех своих работников и привлекаемых для исполнения Договора третьих лиц и обеспечить соблюдение ими указанных процедур и локальных актов.

1.5. Удаленный доступ к информационным системам и элементам информационной сети Предприятия Контрагенту не предоставляется.

2. Права и обязанности Сторон

2.1. Предприятие обязано:

2.1.1. создать персонализированные учетные записи для доступа работников Контрагента к оборудованию с ограниченным сроком действия (срок определяется Предприятием самостоятельно);

2.1.2. обеспечить доступ работникам Контрагента к оборудованию.

2.2. Предприятие имеет право:

2.2.1.проводить контроль использования оборудования работниками Контрагента на территории Предприятия;

2.2.2.в любой момент приостановить, ограничить и полностью закрыть доступ Контрагента к предоставленному оборудованию, в том числе в случае нарушения настоящих Требований со стороны работников Контрагента. При этом Предприятие направляет Контрагенту соответствующее письменное уведомление в течение 1 (одного) дня с момента приостановления/ограничения/прекращения доступа к оборудованию. Приостановление доступа Контрагента к предоставленному оборудованию в случае нарушения настоящих Требований не является основанием для освобождения Контрагента от ответственности за нарушение обязательств по Договору.

2.3.Контрагент обязан:

2.3.1.для создания учетных записей и согласования доступа к оборудованию работникам Контрагента направить Предприятию по электронной почте заполненную «Информационную карточку работника» по следующей форме:

Информационная карточка работника Контрагента	
ФИО работника	
Компания	
Ресурсная роль	
Подтверждение квалификации (сертификаты, специализированные курсы)	
Наименование услуги	
Обслуживаемая система (указывается при необходимости)	
Виды выполняемых работ/оказываемых услуг	
Уровень доступа/права в системе	
Период предоставления доступа	
ФИО заменяемого работника, обоснование замены (указывается при необходимости)	
Дата заполнения	

Работник Контрагента ознакомлен с внутренними процедурами Предприятия, регламентирующими порядок использования оборудования, предоставленного Контрагенту.

2.3.2.соблюдать разделы 3-6 настоящих Требований;

2.3.3.осуществлять замену работников, имеющих допуск к оборудованию, на иных, только по письменному согласованию с Предприятием, с обоснованием причин замены (посредством направления новой информационной карточки работника);

2.3.4.извещать Предприятие не менее чем за 5 (пять) рабочих дней до даты увольнения работника Контрагента или его отстранения от осуществления действий, связанных с использованием предоставленного Контрагенту оборудования;

2.3.5.предоставлять Предприятию возможность осуществлять контроль над работой работников Контрагента с оборудованием, предоставленным Предприятием;

2.3.6.в случае попадания к работникам Контрагента паролей доступа, прав, полномочий и привилегий (умышленного или случайного), отличных от согласованных и выданных

Предприятием, Контрагент не вправе их использовать и обязан незамедлительно сообщить Предприятию об их получении;

2.3.7.в случае порчи (утраты) предоставленного Предприятием оборудования по вине Контрагента, в течение 10 (десяти) рабочих дней с момента обнаружения факта порчи, либо получения письменного требования Предприятием (в зависимости от даты, которая наступит раньше), на основании письменного требования Предприятия, возместить его стоимость Предприятию либо приобрести по согласованию с Предприятием оборудование, являющееся полноценной функциональной заменой, а также возместить все документально подтвержденные расходы, связанные с его доставкой, выполнением работ по приведению его в рабочее состояние (в том числе монтаж, демонтаж и т.д.);

2.3.8. использовать предоставленное оборудование исключительно на территории Предприятия;

2.3.9.не использовать программное обеспечение, установленное на оборудовании, предоставленном Контрагенту, до его предоставления Контрагенту, какими-либо способами, кроме минимально необходимых для исполнения Контрагентом обязательств по Договору, в том числе не копировать, не воспроизводить программное обеспечение, не вносить в него изменения, не производить его анализ или декомпиляцию.

3. Требования по использованию Контрагентом оборудования, предоставленного Предприятием

3.1.Контрагент обязан обеспечить использование предоставленного ему оборудования, персонализированных учетных записей для доступа работников Контрагента к оборудованию, только для исполнения обязанностей по Договору.

3.2.Во время использования оборудования Контрагент обязан обеспечивать физическую безопасность предоставленного ему компьютерного оборудования, не допускать физического повреждения, не предоставлять доступ к оборудованию лицам, не являющимся работниками Контрагента. Принимать пищу, хранить или использовать жидкости вблизи оборудования запрещается.

3.3.Контрагент обязан обеспечить выключение работниками Контрагента персональных компьютеров, предоставленных Контрагенту, предусмотренным для используемой операционной системы способом, если компьютеры не используются 4 (четыре) или более часа подряд, а также блокировку персональных компьютеров предусмотренным для используемой операционной системы способом на время отсутствия работника Контрагента от 15 (Пятнадцати) минут до 4 (четырёх) часов подряд.

3.4.Контрагенту запрещается осуществлять обслуживание или ремонт персональных компьютеров, предоставленных Предприятием, самостоятельно перемещать оборудование, предоставленное Предприятием, нарушать правила эксплуатации компьютерного оборудования, загораживать вентиляционные отверстия, наклеивать картинки и прочие аппликации на монитор и корпус компьютера.

3.5.Контрагенту запрещается изменять время и дату на персональных компьютерах, предоставленных Предприятием.

3.6.Контрагенту запрещается создание и использование любых локальных учетных записей на персональных компьютерах, предоставленных Предприятием.

4.Требования по соблюдению информационной безопасности

4.1. Контрагенту **запрещается:**

4.1.1.передавать другим лицам или разглашать в любой форме персональные атрибуты доступа к оборудованию, предоставленному Предприятием;

4.1.2.самостоятельно подключать, отключать и вносить изменения в конфигурацию оборудования независимо от вида и назначения, если Договором прямо не предусмотрены подобные действия;

4.1.3.преднамеренно записывать, создавать, компилировать, копировать, распространять, запускать на выполнение или пытаться встраивать любые машинные коды, разработанные для самовоспроизводства, повреждения или создания любых других помех функционированию оборудования, предоставленного Предприятием, и нормальной работе других лиц;

4.1.4.самостоятельно приобретать Wi-Fi роутеры, USB-модемы и аналогичное им оборудование и подключать их к персональным компьютерам, входящим в состав оборудования, предоставленного Предприятием;

4.1.5.самостоятельно устанавливать, загружать любые виды программного обеспечения на персональных компьютерах, предоставленных Предприятием, и давать согласие на принятие условий для загрузки программного обеспечения;

4.1.6.осуществлять доступ с персональных компьютеров, входящих в состав оборудования, предоставленного Предприятием, к публичным сервисам электронной почты, файлового обмена, файлового хранения, а также к сервисам развлекательного характера, не имеющим отношения к обязанностям Контрагента по Договору;

4.1.7. устанавливать, запускать, использовать на персональных компьютерах, предоставленных Предприятием, программное обеспечение публичных/внешних сервисов обмена мгновенными сообщениями, аудио и видеосвязи;

4.1.8.размещать и хранить информацию, не имеющую отношения к обязанностям Контрагента по Договору (личную и развлекательного характера, в том числе фильмы, видеоклипы, музыку, игры, личные фотографии) на сетевых ресурсах Предприятия и жестких дисках персональных компьютеров, предоставленных Предприятием;

4.1.9.размещать и хранить информацию, имеющую отношение к обязанностям Контрагента по Договору, а также конфиденциальную информацию на локальных жестких дисках персональных компьютеров, предоставленных Предприятием;

4.1.10.осуществлять неправомерный доступ к охраняемой законом компьютерной информации, если это деяние может повлечь уничтожение, блокирование, модификацию либо копирование компьютерной информации ;

4.1.11.устанавливать, использовать любые программные или аппаратные средства, позволяющие обезличивать, скрывать действия работников Контрагента с оборудованием, предоставленным Предприятием;

4.1.12.устанавливать, использовать любые средства удаленного доступа или управления;

4.1.13.создавать дополнительные каналы выхода в сеть Интернет (к примеру, устанавливать внешние модемы), предпринимать попытки получить доступ в Интернет в обход настроек действующей инфраструктуры и установленных Предприятием правил использования доступа в Интернет;

4.1.14.самостоятельно изменять настройки операционной системы, установленной на компьютерном оборудовании, предоставленном Предприятием.

5. Требования по применению паролей

5.1. Все выбираемые работниками Контрагента пароли доступа к персональным компьютерам, предоставленным Предприятием, должны отвечать приведенным ниже требованиям:

- содержать не менее 8 символов;
- содержать 3 любых вида символов из 4: строчные буквы, заглавные буквы, цифры, спецсимволы;
- не повторять ни один из 24 предыдущих паролей;
- не являться словом из словаря, сленга, диалекта, жаргона;
- не являться личной информацией (к примеру, для создания паролей не должны применяться имена членов семьи, адреса, телефоны, даты рождения);
- не состоять из последовательностей символов раскладок клавиатуры (к примеру, 123456qwerty, 1qaz2wsx).

5.2. Рекомендуется выбрать пароли, в которых будет выполнено хотя бы одно из следующих условий:

- несколько слов написаны слитно;
- при наборе слова на клавиатуре использованы клавиши, смещенные относительно нужных на один ряд вверх, вниз, вправо или влево;
- слово набрано со смещением на определенное количество букв вверх или вниз по алфавиту;
- произвольная комбинация цифр и обычного слова;
- намеренно неправильное написание слова (но не обычная в данном слове орфографическая ошибка).

5.3. Работники Контрагента обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

5.4. Запрещается:

- сообщать или разглашать свой пароль кому-либо, включая коллег, руководителей и работников службы технической поддержки, любыми средствами и способами;
- записывать, хранить пароли учетных записей пользователей в доступной для чтения форме в любом виде;
- использовать автоматическое сохранение пароля;
- использовать общие пароли доступа к персональным компьютерам совместно с другими работниками.

5.5. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого работника Контрагента.

5.6. Все текущие операции с паролем работники Контрагента должны осуществлять лично, не допуская возможности рассмотреть состав вводимого пароля и порядок введения символов.

5.7. Формы ввода пароля должны скрывать вводимые символы.

5.8. Работникам Контрагента запрещается предпринимать какие-либо действия по получению (раскрытию) паролей не принадлежащих им учетных записей.

6. Требования по антивирусной безопасности

6.1. Работникам Контрагента запрещается:

- деинсталляция или деактивация антивирусного ПО, а также изменение его настроек на персональных компьютерах, предоставленных Предприятием;
- создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

6.2. Перечень правил по минимизации рисков заражения вредоносным ПО:

Во избежание заражения оборудования вредоносным ПО Контрагент обязан обеспечить соблюдение всеми работниками Контрагента следующих правил:

6.2.1. В случае сомнений в наличии или в корректной работе на компьютере антивирусного ПО необходимо незамедлительно сообщить об этом Предприятию.

6.2.2. Запрещается открывать какие-либо файлы, находящиеся во вложениях к электронным письмам, которые отправлены с подозрительных или неизвестных работнику Контрагента адресов, пересылать их другим адресатам. В случае получения таких писем следует немедленно их удалить из папки «Входящие», а затем удалить их из папки «Удаленные» для того, чтобы исключить возможность их восстановления.

6.2.3. В случае возникновения подозрений на наличие зараженных файлов во вложениях к сообщениям электронной почты (к примеру, подозрительные имена или расширения файлов вложений, подозрительный источник сообщения, неизвестный отправитель с адресом электронной почты публичного почтового сервиса), которые однако могут быть полезны работнику Контрагента, необходимо незамедлительно сообщить об этом Предприятию для проведения проверки подозрительного сообщения.

6.2.4. Запрещается загружать файлы и соглашаться на предложения загрузить или установить ПО с неизвестных работнику Контрагента Интернет сайтов. В случае возникновения сомнений в благонадежности сайта, но при необходимости дальнейшей с ним работы, необходимо обратиться к Предприятию для проведения проверки.

6.2.5. Запрещается использовать на рабочих местах съемные носители информации, если эти носители получены из неизвестных или подозрительных источников или могли использоваться на других компьютерах, возможно, не защищенных антивирусными программами. В случае необходимости следует обратиться к Предприятию для проведения соответствующих проверок.

6.2.6. В случае обнаружения признаков заражения компьютера вредоносным ПО (включая значительное увеличение времени отклика компьютера на действия пользователя, появление сообщения об ошибках, необъяснимая потеря файлов, изменение дат обновления файлов, увеличение размера файлов, системные сбои (включая случаи, когда операционная система перестает загружаться), а также любые другие изменения в работе компьютера). Незамедлительно сообщать об этом Предприятию. Это позволит минимизировать ущерб,

наносимый компьютерным вирусом, и принять необходимые меры для предотвращения повторного заражения.

7. Предоставление, изменение и прекращение полномочий доступа

7.1.Обращения по предоставлению или изменению доступа для работников Контрагента должны согласовываться уполномоченными работниками Предприятия, которые в свою очередь должны проанализировать обоснованность предоставления доступов.

7.2.Обращения по предоставлению, изменению и блокировке доступа должны быть согласованы Предприятием. При рассмотрении обращений уполномоченные работники Предприятия имеют право запросить и получить любую необходимую информацию по обращению, а так же отклонить обращение без обоснования причин.

7.3.Предприятие имеет право в любой момент ограничить либо заблокировать доступ как отдельным работникам Контрагента, так и всем работникам Контрагента.

8. Ответственность Контрагента

8.1.При обнаружении фактов нарушения настоящих Требований уполномоченный работник функции экономической безопасности Предприятия составляет акт о нарушении в присутствии нарушителя и непосредственного руководителя (старшего группы, бригадира и т.п.) нарушителя. Акт в данном случае подписывается сотрудником Предприятия, нарушителем и его непосредственным руководителем (старшим группы, бригадиром и т.п.).

8.2.При отказе нарушителя и/или непосредственного руководителя (старшего группы, бригадира и т.п.) нарушителя подписать акт, а также в случае отсутствия в момент составления акта непосредственного руководителя (старшего группы, бригадира и т.п.) нарушителя, акт подписывается комиссионно, в составе не менее трех человек, сотрудниками Предприятия. При этом в акте делается соответствующая запись об отказе от подписания или об отсутствии непосредственного руководителя (старшего группы, бригадира и т.п.) нарушителя. В последующем о случившемся информируется руководство Контрагента.

8.3.Несоблюдение работником Контрагента настоящих Требований дает Предприятию право требовать уплаты штрафа от Предприятия в соответствии с указанным в настоящем пункте перечнем штрафных санкций за нарушения Требований путем перечисления подлежащей уплате суммы штрафа на расчетный счет Предприятия в течение 10 (десяти) рабочих дней с момента направления письменного обращения Предприятием. В случае невыплаты Контрагентом таких штрафов в указанный срок сумма, подлежащая оплате Контрагентом, может быть уменьшена Предприятием на сумму всех штрафов и неустоек, а также иных сумм, предъявленных Предприятием в претензиях. Размер штрафа определяется исходя из нижеуказанных данных таблицы.

№ п/п	Наименование нарушения, за каждый факт совершения которого Контрагент уплачивает Предприятию штраф	Сумма штрафных санкций, тыс. руб.
1	Нарушение Требований по использованию Контрагентом оборудования, предоставленного Предприятием (раздел 3 настоящих Требований)	50
2	Нарушение Требований по соблюдению информационной безопасности (раздел 4 настоящих Требований)	50

3	Нарушение Требований по применению паролей (раздел 5 настоящих Требований)	50
4	Нарушение Требований по антивирусной безопасности (раздел 6 настоящих Требований)	50

**Приложение №1 к Требованиям о предоставлении оборудования
для целей исполнения обязанностей по Договору**

**Форма Акта приема-передачи оборудования
для целей исполнения обязанностей по Договору**
№ _____ от «___» _____ 20__ года

г. _____ «___» _____ 20__ г.

Публичное акционерное общество «СИБУР Холдинг» (ПАО «СИБУР Холдинг»)/ Предприятие Группы СИБУР (полное и сокращенное наименование), именуемое в дальнейшем «Предприятие», в лице _____, действующего на основании _____, с одной стороны, и _____ *(полное и сокращенное наименование)*, именуемое далее «Контрагент», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые «Стороны», составили настоящий Акт приема-передачи оборудования о нижеследующем:

1. Во исполнение Договора № _____ от «___» _____ 20__ года Предприятие передало, а Контрагент принял для целей исполнения обязанностей по Договору следующее оборудование:

_____ *(указать наименование оборудования, его марку, модель, год выпуска, инвентарный, заводской/серийный номера, а также иные индивидуализирующие признаки)* (далее по тексту – «оборудование»).

2. Оборудование, указанное в п. 1 настоящего Акта, передается Контрагенту в следующей комплектации: *(далее указать комплектацию передаваемого оборудования)*.

3. Вместе с оборудованием Предприятие передало:

3.1. _____

3.2. _____ *(указать техническую документацию на оборудование, ее номер, дату, кем выдана; материалы и комплектующие Предприятия)*

4. Настоящий Акт составлен в двух экземплярах, имеющих одинаковую юридическую силу.

Контрагент:

Предприятие:

_____ *(Наименование Контрагента)*

_____ *(Наименование Предприятия)*

_____ *(ФИО подписанта)*

_____ *(ФИО подписанта)*