Соглашение об обмене электронными документами между Министерством финансов Челябинской области и участником юридически значимого электронного документооборота

г. Челябинск «18» марта 2022 г.

Министерство финансов Челябинской области в лице начальника отдела специальных технических средств Повышева Александра Александровича, действующего на основании приказа Министерства финансов Челябинской области от 01.07.2021г. № 01/5-109, именуемое в дальнейшем «Организатор», с одной стороны, и

Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад № 1 г. Челябинска»

(полное наименование организации в соответствии с учредительным документом)

в лице Заведующего Шавейниковой Юлии Юрьевны,

(должность, ФИО руководителя)

действующего на основании Устава, именуемое в дальнейшем «Участник», с другой стороны, заключили настоящее Соглашение о нижеследующем.

1. Термины и понятия, используемые в настоящем Соглашении

1.1. Такие термины и понятия, как «квалифицированный сертификат ключа проверки электронной подписи» (далее – сертификат), «ключ электронной подписи» (далее – ключ), «усиленная квалифицированная электронная подпись» (далее – ЭП) и «электронный документ», используемые в настоящем Соглашении, применяются в том же значении, что и в Федеральном законе от 06.04.2011 № 63-ФЗ «Об электронной подписи» (далее – 63-ФЗ).

1.2. Автоматизированная система Министерства финансов Челябинской области – программный комплекс, предназначенный для автоматизации бюджетного процесса в Челябинской области (далее – Система).

Клиентская часть Системы – аппаратно-программный комплекс, предназначенный для хранения, обработки и передачи данных по телекоммуникационным каналам связи с рабочих машин уполномоченных лиц на серверную часть Системы.

Компрометация ключа – нарушение конфиденциальности ключа ЭП: использование ключа ЭП без согласия владельца, а так же хищение, утеря, искажение, несанкционированное копирование или другие нарушения сохранения тайны и целостности ключа ЭП.

Юридически значимый электронный документооборот (далее – ЮЗЭД) – документооборот на базе Системы, в котором стороны совершают действия по принятию к исполнению электронных документов, удостоверенных ЭП, и при этом несут ответственность за совершение либо несовершение этих действий.

Организатор – Министерство финансов Челябинской области, являющееся стороной ЮЗЭД (в лице уполномоченных лиц) на базе Системы, а также организатором ЮЗЭД в Системе, осуществляющим функции по хранению на своём оборудовании базы данных и конфигурации серверной части Системы, по настройке Системы на серверных станциях.

Регламент применения электронной подписи сторонами юридически значимого электронного документооборота (далее – Регламент) – утверждённый Организатором документ, определяющий статусы электронных документов, на которых происходит наложение ЭП.

Удостоверяющий центр (далее – УЦ) – аккредитованный УЦ, осуществляющий функции по созданию и выдаче Участникам и сотрудникам Министерства финансов Челябинской области сертификатов, а также иные функции аккредитованного УЦ, предусмотренные 63-ФЗ в соответствии с Порядком работы УЦ.

Порядок работы УЦ – утверждённый УЦ Порядок реализации функций аккредитованного удостоверяющего центра и исполнения его обязанностей, определяющий порядок работы УЦ.

Реестр Системы – справочник Системы, в котором хранится перечень сертификатов уполномоченных лиц сторон.

Серверная часть Системы – аппаратно-программный комплекс, предназначенный для хранения, обработки и передачи данных по телекоммуникационным каналам связи на клиентские части Системы.

Средства криптографической защиты информации (далее – СКЗИ) – аппаратно-программный комплекс, выполняющий функцию по созданию ЭП, а также обеспечивающий защиту информации по утверждённым стандартам и сертифицированный в соответствии с законодательством.

Статус электронного документа – атрибут электронного документа, идентифицирующий его состояние по определённому признаку.

Участник – юридическое лицо, заключившее соглашение об обмене электронными документами с Министерством финансов Челябинской области для участия в ЮЗЭД.

Уполномоченное лицо – должностное лицо Участника или Организатора, действующее от имени Участника или Организатора, наделенное правом использования электронной подписи.

Сторона – Организатор и (или) Участник (при участии в ЮЗЭД).

Экспертная комиссия – комиссия, разрешающая конфликтные ситуации, связанные с использованием ЮЗЭД.

2. Предмет настоящего Соглашения

2.1. Настоящее Соглашение определяет условия и порядок обмена юридически значимыми электронными документами между сторонами на базе Системы.

2.2. Настоящее Соглашение определяет права и обязанности сторон, возникающие при обмене юридически значимыми электронными документами на базе Системы.

3. Общие положения

3.1. Стороны осуществляют обмен юридически значимыми электронными документами, не содержащими конфиденциальных сведений и сведений, составляющих государственную тайну, на базе Системы с использованием телекоммуникационных каналов связи.

3.2. С целью обеспечения авторства и целостности электронных документов при информационном взаимодействии стороны используют сертифицированные СКЗИ.

3.3. Выдача сертификатов осуществляется УЦ в соответствии с Порядком работы УЦ.

3.4. Используемые при информационном взаимодействии сторон электронные документы с ЭП, сформированной сторонами средствами СКЗИ, имеют равную юридическую силу с документами на бумажном носителе, подписанными соответствующими собственноручными подписями уполномоченных лиц сторон и скреплёнными оттисками печатей (независимо от того существуют такие документы на бумажных носителях или нет).

3.5. Стороны признают, что СКЗИ, которые используются при обмене юридически значимыми электронными документами в Системе и реализуют функции создания ЭП, достаточны для подтверждения следующего:

1) электронный документ исходит от одной из сторон (уполномоченного лица), его передавшего (подтверждение авторства электронного документа);

2) электронный документ не претерпел изменений в процессе передачи между сторонами (подтверждение целостности и подлинности электронного документа).

3.6. Стороны признают, что скан-копии писем Министерства финансов Челябинской области на официальном бланке Министерства финансов Челябинской области, носящие характер информационного сообщения, направленные Участнику с использованием Системы, являются официальными сообщениями Министерства финансов Челябинской области.

4. Права и обязанности

4.1. Организатор обязан:

4.1.1. Обеспечить функционирование необходимого аппаратно-программного комплекса серверной части Системы, а также клиентской части Системы уполномоченных лиц Организатора для предоставления Участнику возможности обмена юридически значимыми электронными документами между сторонами.

4.1.2. Соблюдать требования приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (далее – Инструкция N 152).

4.1.3. Соблюдать Требования к обеспечению информационной безопасности участника электронного взаимодействия (Прилагается).

4.1.4. Соблюдать Порядок подключения автоматизированного рабочего места участника электронного взаимодействия к Автоматизированной системе Министерства финансов Челябинской области, утверждённый Организатором.

4.1.5. При изменении Порядка подключения автоматизированного рабочего места участника электронного взаимодействия к Автоматизированной системе Министерства финансов Челябинской области произвести настройки на серверной части Системы и оповестить по телекоммуникационным каналам связи Участника об этих изменениях.

4.1.6. В случае необходимости (необходимость устанавливается Организатором) обеспечить необходимыми СКЗИ уполномоченных лиц Участника.

4.1.7. Немедленно уведомить Участника любым доступным способом:

– об ошибках в работе Системы, возникающих при работе с ЭП (подписание ЭП, проверка ЭП и др.);

– об ошибках, возникающих в связи с попытками нарушения информационной безопасности;

– о возникновении сбоев, неисправностей и отказов оборудования;

– о возникновении сбоев и ошибок программного обеспечения;

– о возникновении сбоев, неисправностей и отказов систем связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения и согласовать свои дальнейшие действия.

4.1.8. Вести актуальный реестр Системы.

4.1.9. Прекратить использование сертификатов уполномоченных лиц сторон в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о факте компрометации ключа.

4.1.10. Хранить материальные носители, содержащие ключи уполномоченных лиц Организатора, в месте, исключающем доступ неуполномоченных лиц и (или) возможность повреждения материальных носителей.

4.2. Участник обязан:

4.2.1. Обеспечить функционирование аппаратно-программного комплекса клиентской части уполномоченных лиц Участника для обеспечения работоспособности ЮЗЭД (требования к аппаратно-программному комплексу клиентской части Системы указаны в документации к Системе).

4.2.2. Соблюдать требования Инструкции N 152.

4.2.3. Соблюдать Требования к обеспечению информационной безопасности участника электронного взаимодействия (Прилагается).

4.2.4. Получать сертификаты в УЦ в соответствии с Порядком работы УЦ.

4.2.5. В целях обеспечения безопасности обработки и передачи юридически значимых электронных документов:

– соблюдать требования эксплуатационной документации на используемые СКЗИ;

– не допускать появления в аппаратно-программном комплексе Системы компьютерных вирусов;

– прекращать использование скомпрометированного ключа ЭП и немедленно информировать Организатора и УЦ о факте компрометации ключа;

– в случае утери СКЗИ приобрести за свой счет СКЗИ, совместимое с информационными системами Министерства финансов Челябинской области. Акт установки СКЗИ представить в Министерство финансов Челябинской области в срок не позднее 30 календарных дней с момента утери СКЗИ.

4.2.6. Соблюдать Порядок подключения автоматизированного рабочего места участника электронного взаимодействия к Автоматизированной системе Министерства финансов Челябинской области, утверждённый Организатором.

4.2.7. Обработать электронный документ в соответствии с Регламентом при условии соответствия электронных документов признакам и требованиям к юридически значимым электронным документам (признаки и требования указаны в Регламенте).

4.2.8. Хранить материальные носители, содержащие ключи ЭП уполномоченных лиц Участника, в месте, исключающем доступ неуполномоченных лиц и (или) возможность повреждения материальных носителей.

4.2.9. Немедленно известить Организатора о приостановлении исполнения своих обязанностей в случае невозможности исполнения обязательств по настоящему Соглашению.

4.2.10. Руководствоваться порядком разрешения конфликтных ситуаций, утверждённым Организатором, при возникновении споров, связанных с принятием или непринятием и (или) с исполнением или неисполнением электронных документов, подписанных ЭП, входящих в перечень юридически значимых электронных документов в соответствии с Регламентом.

4.2.11. По первому обоснованному требованию предоставить Организатору бумажные копии выгруженных из Системы электронных документов, входящих в перечень юридически значимых электронных документов в соответствии с Регламентом.

4.2.12. Заменить сертификат в порядке и в случаях, предусмотренных Порядком работы УЦ.

4.2.13. Немедленно уведомить Организатора любым доступным способом:

– о компрометации ключа;

– об изменении состава уполномоченных лиц Участника, обладающих правом использования ключей;

– об ошибках в работе Системы, возникающих при работе с ЭП (подписание ЭП, проверка ЭП и др.);

– об ошибках, возникающих в связи с попытками нарушения информационной безопасности;

– о возникновении сбоев, неисправностей и отказов оборудования;

– о возникновении сбоев и ошибок программного обеспечения;

– о возникновении сбоев, неисправностей и отказов систем связи, энергоснабжения, кондиционирования и других систем жизнеобеспечения и согласовать свои дальнейшие действия.

4.2.14. Использовать СКЗИ, реализующие функции создания ЭП при обмене юридически значимыми электронными документами в Системе, которые имеют действующий сертификат соответствия требованиям ФСБ России.

4.2.15. Регулярно проверять наличие входящих сообщений в Системе, направленных от имени Организатора.

4.3. В случае несоответствия электронного документа признакам и требованиям к юридически значимым электронным документам в соответствии с Регламентом, а также в случае угрозы несанкционированного доступа к программно-аппаратным комплексам сторон, Участник вправе отказаться от обработки электронного документа, уведомив об этом Организатора по телекоммуникационным каналам связи с указанием причины отказа.

5. Порядок подключения к ЮЗЭД

5.1. Участник в течение пяти рабочих дней после подписания настоящего Соглашения выполняет подключение автоматизированных рабочих мест участника в соответствии с Порядком подключения автоматизированного рабочего места участника электронного взаимодействия к Автоматизированной системе Министерства финансов Челябинской области, утверждённым Организатором.

5.2. Организатор в течение трёх дней после получения на адрес электронной почты cert@minfin74.ru от Участника сертификатов уполномоченных лиц Участника вводит в действие эти сертификаты.

5.3. Организатор оповещает по телекоммуникационным каналам связи Участника о готовности серверной части Системы, клиентской части Системы и уполномоченных лиц Организатора к вводу в действие ЮЗЭД.

6. Ответственность

6.1. Стороны несут ответственность за действия своих уполномоченных лиц при осуществлении обмена юридически значимыми электронными документами в рамках настоящего Соглашения.

6.2. За неисполнение или ненадлежащее исполнение своих обязательств по настоящему Соглашению стороны несут ответственность в соответствии с законодательством Российской Федерации.

6.3. При использовании телекоммуникационных каналов связи и передаче данных стороны не несут ответственность за возможные временные задержки (произошедшие не по их вине) при доставке юридически значимых электронных документов.

7. Разрешение конфликтных ситуаций

7.1. Все споры и разногласия, которые могут возникнуть в связи с исполнением настоящего Соглашения, стороны будут стремиться разрешить путём переговоров.

7.2. В случаях, если конфликтная ситуация не урегулирована, стороны обращаются в Арбитражный суд Челябинской области.

8. Форс-мажорные обстоятельства

8.1. Стороны не несут ответственность за невыполнение, несвоевременное или ненадлежащее исполнение какого-либо обязательства по настоящему Соглашению, если указанное невыполнение, несвоевременное или ненадлежащее исполнение обусловлены исключительно наступлением и (или) действием обстоятельств непреодолимой силы, независящих от воли сторон, которые стороны не могли ни предвидеть, ни предотвратить (далее – форс-мажорные обстоятельства).

8.2. Сторона, надлежащее исполнение обязательств которой оказалось невозможным в силу влияния форс-мажорных обстоятельств, в течение 3 (трёх) рабочих часов после их наступления информирует другую сторону о наступлении этих обстоятельств и об их последствиях любым доступным способом и принимает все возможные меры с целью максимального ограничения отрицательных последствий, вызванных форс-мажорными обстоятельствами.

8.3. Неизвещение или несвоевременное извещение другой стороны стороной, надлежащее исполнение обязательств которого оказалось невозможным в силу влияния форс-мажорных обстоятельств, о наступлении этих обстоятельств, влечёт за собой утрату права ссылаться на эти обстоятельства.

8.4. Наступление форс-мажорных обстоятельств может вызвать увеличение срока исполнения обязательств по настоящему Соглашению на период их действия, если стороны не договорились об ином.

9. Срок действия настоящего Соглашения

9.1. Настоящее Соглашение вступает в силу с момента его подписания сторонами и действует до момента его расторжения в установленном порядке.

9.2. Дата начала обмена юридически значимыми электронными документами определяется датой оповещения Организатором о готовности серверной части Системы, клиентской части Системы и уполномоченных лиц Организатора к вводу в действие ЮЗЭД (пункт 5.3 настоящего Соглашения).

10. Прочие условия

10.1. Настоящее Соглашение составлено в двух экземплярах, имеющих равную юридическую силу, по одному экземпляру для Организатора и Участника.

10.2. Все изменения к настоящему Соглашению действительны в том случае, если они оформлены в письменном виде и подписаны уполномоченными представителями сторон.

10.3. Расторжение настоящего Соглашения не влияет на действительность и порядок действия юридически значимых электронных документов, подписанных ЭП уполномоченных лиц сторон до даты его расторжения.

11. Адреса, реквизиты и подписи

Организатор	Участник
Министерство финансов Челябинской области. Юридический и почтовый адрес: 454091, г. Челябинск, пр. Ленина 57 ИНН 7453136570, КПП 745301001, ОГРН 1047424532968, ОКВЭД 75.11.21	Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад № 1 г. Челябинска» Юридический адрес: 454021, г. Челябинск ул. Братьев Кашириных 106-А Почтовый адрес: 454021, г. Челябинск ул. Братьев Кашириных 106-А ИНН 7447033143 КПП 744701001 ОГРН 1027402336741
Начальник отдела специальных технических средств	Заведующий
_____ А.А. Повышев	_____ Ю.Ю. Шавейникова
М.П.	М.П.

Приложение
к Соглашению об обмене электронными документами
между Министерством финансов Челябинской области
и участником юридически значимого электронного
документооборота

Требования
к обеспечению информационной безопасности участника электронного взаимодействия

1. Термины и определения

Участник - участник электронного взаимодействия, под которым понимаются:

главные распорядители средств областного бюджета, заключившие Соглашение об обмене электронными документами между Минфином и участником юридически значимого электронного документооборота (далее – Соглашение);

распорядители и получатели средств областного бюджета, областные бюджетные учреждения и областные автономные учреждения, заключившие Соглашение;

финансовые органы муниципальных образований Челябинской области, заключившие Соглашение;

главные распорядители, распорядители и получатели средств местных бюджетов области, муниципальные бюджетные учреждения и муниципальные автономные учреждения, заключившие Соглашение;

юридические лица, которым из областного бюджета предоставляются субсидии (за исключением областных бюджетных учреждений и областных автономных учреждений), и заключившие Соглашение;

органы местного самоуправления Челябинской области, заключившие Соглашение;

распорядители и получатели средств местных бюджетов области, муниципальные бюджетные учреждения и муниципальные автономные учреждения.

АРМ Участника - Автоматизированное рабочее место Участника, представляющее собой персональный компьютер и подключенное к нему периферийное оборудование;

Защищаемая информация - подлежащая защите информация, обрабатываемая на АРМ Участника.

2. Требования к режиму информационной безопасности

Защищаемая информация может включать следующие сведения:

- персональные данные сотрудников Участника в составе сертификата электронной подписи, предусмотренные Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

- другие персональные данные физических лиц, получающих денежные средства из бюджета Челябинской области (ФИО, сведения о суммах заработной платы, субсидиях, пособиях, социальных и других выплатах и платежах, номер лицевого банковского счёта);

- сведения о расчётных операциях с использованием средств областного бюджета, средствах, полученных от приносящей доход деятельности, средствах, размещенных на возвратной основе и другие сведения;

В целях организации режима информационной безопасности Участник самостоятельно определяет перечень сведений, составляющих Защищаемую информацию, в соответствии с требованиями законодательства в сфере информационной безопасности, требованиями организаций – учредителей и настоящими Требованиями.

3. Требование к кадровому обеспечению

Участником должен быть назначен администратор информационной безопасности, в должностные обязанности которого входит обеспечение выполнения требований законодательства в сфере информационной безопасности на АРМ Участника, и ответственный за организацию обработки персональных данных.

Администратор безопасности обеспечивает защиту автоматизированного рабочего места в соответствии с требованиями законодательства в области информационной безопасности. Ответственный за организацию обработки персональных данных осуществляет функции, предусмотренные Федеральным Законом от 27.07.2006 N 152-ФЗ «О персональных данных».

4. Требования к размещению технических средств

При размещении в помещениях Участника технических средств, обрабатывающих Защищаемую информацию, в том числе АРМ Участника, должны быть приняты меры по исключению несанкционированного доступа (далее – НСД) в эти помещения.

Средства защищённого хранения ЭП требуется учитывать в Журнале учёта средств криптографической защиты информации и хранить в надёжно запираемых металлических шкафах или сейфах в соответствии с требованиями Приказа Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. N 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» (далее – Инструкция N 152).

5. Требования по допуску лиц к АРМ Участника

К АРМ Участника допускаются лица, ознакомленные с настоящими Требованиями, а также инструктивными материалами Участника в сфере информационной безопасности.

6. Особенности установки программного обеспечения на АРМ Участника

При установке программного обеспечения на АРМ Участника необходимо соблюдать следующие требования:

1) использование только лицензионного программного обеспечения;

2) установку программных средств обработки и защиты Защищаемой информации необходимо производить только из доверенного источника;

3) на АРМ Участника не должны устанавливаться средства разработки и отладки программного обеспечения;

4) АРМ Участника не должен содержать программное обеспечение, не относящееся к деятельности сотрудника его эксплуатирующего;

5) перед установкой программное обеспечение должно пройти антивирусный контроль;

6) не допускается установка на АРМ Участника неактуальных и неподдерживаемых версий программного обеспечения;

7) требуется периодически проводить контроль целостности СКЗИ, установленного на АРМ Участника.

7. Требования по защите от НСД при эксплуатации АРМ Участника

При организации работ по защите информации от НСД Участнику необходимо соблюдать следующие требования:

1) исключить возможность удаленного управления, администрирования и модификации АРМ Участника и его настроек;

2) разработать и применить политику назначения и смены паролей для входа в операционную систему с учётом следующих правил:

длина пароля должна быть не менее 8-ми символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

пароль не должен включать в себя легко вычисляемые сочетания символов (даты рождения, имена, фамилии и т. д.), а также общепринятые сокращения;

пользователь не имеет права передавать\сообщать свой пароль другим лицам;

периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев. Число неудачных попыток ввода пароля должно быть ограничено числом 10;

3) средствами BIOS должна быть исключена возможность работы на АРМ Участника, если во время его начальной загрузки не проходят встроенные тесты;

4) запрещено оставлять АРМ Участника без блокировки сеанса пользователя;

5) не допускается осуществлять несанкционированное копирование ключевых носителей информации (при санкционированном руководителем Участника копировании должны соблюдаться требования Инструкции № 152);

6) запрещено разглашать содержимое носителей ключевой информации или передавать носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и иные средства отображения информации, записывать на ключевые носители постороннюю информацию;

7) пользователи АРМ Участника должны иметь минимально возможные для нормальной работы права доступа;

8) требуется регулярно устанавливать пакеты обновления безопасности операционной системы и прикладного программного обеспечения, обновлять антивирусные базы средств антивирусной защиты, проводить контроль на отсутствие компьютерных вирусов всех сменных и подключаемых носителей (CD-дисков, DVD-дисков, USB-флеш накопителей и т.п.);

9) исключить одновременную работу операционной системы с загруженной ключевой информацией нескольких пользователей;

10) наличие только одной операционной системы на АРМ Участника;

11) участник должен принять меры, исключающие несанкционированное вскрытие корпуса АРМ Участника.