СОГЛАШЕНИЕ
об электронном документообороте № 22-277/53/34-Э

г. Москва «23» августа 2019 г.

Банк ВТБ (публичное акционерное общество), именуемый в дальнейшем «Банк», в лице руководителя Департамента брокерского обслуживания – старшего вице-президента, Потапова Владимира Михайловича, действующего на основании Доверенности № 350000/920-ДН от 26.02.2019 г., с одной стороны и **Общество с ограниченной ответственностью ВТБ Капитал Пенсионный резерв**, именуемое в дальнейшем «Контрагент» в лице Генерального директора Волгина Олега Николаевича, действующей на основании Устава, с другой стороны, вместе далее именуемые «Стороны», заключили настоящее Соглашение о нижеследующем:

1. ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ

1.1. **Владелец Сертификата** – Уполномоченное лицо Банка или Контрагента, которому в установленном Договором и настоящим Соглашением порядке выдан Сертификат.

1.2. **Запрос на сертификат** - информационный массив, содержащий **Ключ проверки электронной подписи** Уполномоченного лица Банка или Контрагента, информацию об этом Уполномоченном лице, а также некоторую вспомогательную информацию, на основе которого формируется Сертификат

1.3. **Ключ проверки электронной подписи** - уникальная последовательность символов, однозначно связанная с Ключом электронной подписи и предназначенная для проверки подлинности электронной подписи

1.4. **Ключ электронной подписи** - уникальная последовательность символов, предназначенная для создания электронной подписи.

1.5. **Ключ шифрования** - уникальная последовательность символов, предназначенная для криптографического преобразования информации в целях сокрытия ее от посторонних лиц.

1.6. **Ключевая информация** - совокупность Криптографических ключей, Сертификатов и других ключевых документов, однозначно связанных с Ключом электронной подписи

1.7. **Компрометация ключей** – утрата доверия к тому, что используемые Криптографические ключи обеспечивают безопасность информации. К событиям, связанным с компрометацией ключей относятся, включая, но не ограничиваясь следующими:

- Утрата (хищение) носителей ключевой информации, в том числе с последующим их обнаружением
- Увольнение сотрудников, имевших доступ к ключевой информации
- Передача Криптографических ключей по линии связи в открытом виде
- Нарушение правил хранения и уничтожения Криптографических ключей.
- Возникновение подозрений на несанкционированный доступ (или хищение) со стороны третьих лиц к Ключевому носителю
- Вскрытие фактов утечки шифрованной информации или её искажения (подмены, подделки).
- Иные обстоятельства, прямо или косвенно свидетельствующие о наличии возможности несанкционированного доступа к Криптографическим ключам третьих или неуполномоченных лиц.

1.8. **Криптографические ключи** – Ключ электронной подписи, ключи шифрования.

1.9. **Носитель ключевой информации (Ключевой носитель)** – Физический носитель, предназначенный для хранения на нем Ключевой информации. В качестве Ключевого носителя могут применяться отчуждаемые носители (USB Flash Hard Drive, USB-ключи, флоппи диски (дискеты) и т.п.) или непосредственно сам компьютер (на жестком диске данного компьютера: Windows Registry, файловые папки и т.п.)

1.10. **Подтверждение подлинности Электронной подписи в электронном документе** - Положительный результат проверки соответствующим средством электронной подписи с использованием Сертификата принадлежности электронной подписи в электронном документе Владельцу сертификата и отсутствия искажений в подписанном данной электронной подписью электронном документе.

1.11. **Сертификат ключа проверки электронной подписи (Сертификат)** - электронный документ или документ на бумажном носителе, выданные Банком Уполномоченному лицу Контрагента и подтверждающие принадлежность Ключа проверки электронной подписи Владельцу Сертификата.

1.12. **Средство защиты информации (СЗИ)** – Программное обеспечение «File-Pro», обеспечивающее защиту файла с помощью криптографических методов (шифрование/расшифрование, формирование/проверка электронных подписей) файлов или группы файлов, а также программа «Admin PKI», предназначенная для формирования Ключей электронной подписи, Ключей проверки ЭП и Запросов на Сертификат. Указанные программные средства разработаны компанией ЗАО «Сигнал-КОМ» и выполнены с использованием средства криптографической защиты информации «Крипто-КОМ», сертифицированным ФСБ России

1.13. **Уполномоченное лицо Банка** - физическое лицо, полномочия которого выполнять действия, предусмотренные Договором и настоящим Соглашением, подтверждены в соответствии с положениями законодательства Российской Федерации.

1.14. **Уполномоченное лицо Контрагента** - физическое лицо, полномочия которого выполнять действия, предусмотренные Договором и настоящим Соглашением, подтверждены в соответствии с положениями законодательства Российской Федерации.

1.15. **Шифрование** – криптографическое преобразование данных, позволяющее предотвратить доступ неуполномоченных лиц к содержимому зашифрованного электронного документа.

1.16. **Электронный документ** – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах

1.17. **Электронный документооборот (ЭДО)** – передача и прием документов в электронном виде между Сторонами.

1.18. **Электронная подпись (ЭП)** - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. ПРЕДМЕТ СОГЛАШЕНИЯ

2.1. Стороны соглашаются использовать ЭДО при передаче Электронных документов в рамках Договора поручения на осуществление агентской деятельности № 22-277/53/34 от 16.03.2004. Организатором ЭДО является Банк.

2.2. Стороны используют для передачи и приема Электронных документов в сети Интернет электронную почту. В случае технической невозможности передачи и приема электронных документов посредством сети Интернет Стороны осуществляют передачу и прием документов на съемных носителях в виде Электронных документов или в виде документов на бумажных носителях.

2.3. Стороны соглашаются использовать для подтверждения авторства, подлинности и целостности передаваемых Электронных документов Электронную подпись, а также использовать для защиты передаваемых Электронных документов от несанкционированного доступа их Шифрование.

2.4. Стороны признают, что используемые для осуществления ЭДО СЗИ достаточны для подтверждения авторства, подлинности и целостности Электронных документов, также для защиты их от несанкционированного доступа

2.5. Стороны признают, что Электронная подпись, сформированная СЗИ и применяемая в системе ЭДО, соответствует всем признакам и требованиям, предъявляемым к усиленной неквалифицированной электронной подписи, предусмотренным Федеральным законом от 06.04.2011 No63-ФЗ «Об электронной подписи»

2.6. Стороны признают, что получение Электронного документа, подписанного подлинной Электронной подписью Уполномоченного лица в соответствии с условиями Договора и настоящего Соглашения, юридически эквивалентно получению идентичного по смыслу и содержанию документа, составленного на бумажном носителе, подписанного собственноручной подписью Уполномоченного лица и скрепленного печатью.

2.7. Банк осуществляет деятельность по организации защищенного электронного документооборота с применением Электронной подписи на основании имеющейся у него лицензии ФСБ России.

2.8. Участники систем защищенного электронного документооборота осуществляют эксплуатацию программного обеспечения СЗИ в рамках лицензий, имеющихся у Банка, как организатора системы электронного документооборота.

3. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

3.1. Полномочия должностных лиц Сторон по генерации Криптографических ключей, обмену Сертификатами и формированию Электронной подписи, передаваемых электронных документов, определяются внутренними нормативными документами Сторон.

3.2. Стороны самостоятельно и за свой счет обеспечивают технические, программные и коммуникационные ресурсы, необходимые для организации передачи и приема электронных документов в соответствии с настоящим Соглашением, в том числе:

3.2.1. Персональный компьютер с установленной операционной системой Windows и программой отправки и приема электронной почты.

3.2.2. Подключение к сети Интернет с возможностью приема-передачи сообщений электронной почты.

3.3. Для обмена сообщениями в рамках ЭДО Стороны обязуются использовать адреса электронной почты, указанные в Сертификатах Уполномоченных лиц Банка и Контрагента. В случае необходимости смены адреса электронной почты Стороны обязуются уведомлять об изменениях не позднее чем за один рабочий день до внесения таких изменений. Заявление о смене адреса электронной почты должно быть подписано руководителем организации Контрагента.

3.4. Программное обеспечение, обеспечивающее защиту информации, предоставляется Банком в течение 5 рабочих дней после подписания настоящего Соглашения. Информация о порядке предоставления дистрибутива опубликована на сайте Банка в разделе ПО для электронного документооборота: http://www.vtb.ru/company/programs/setup/

3.5. Стороны осуществляют формирование Криптографических ключей и обмен Сертификатами в следующем порядке:

3.5.1. Стороны самостоятельно формируют с помощью программного обеспечения СЗИ (используется «Admin-PKI») Криптографические ключи.

3.5.2. Запрос на Сертификат в виде файла Контрагент передает в Банк *посредством его отправки по электронной почте на адреса Уполномоченных лиц Банка.*

3.5.3. Банк формирует Сертификаты Уполномоченных лиц Банка и Контрагента, распечатывает их в двух экземплярах (Приложение № 2 к настоящему Соглашению), заверяет подписью уполномоченного должностного лица и скрепляет печатью.

3.5.4. Банк передает Контрагенту Сертификат Уполномоченного лица Контрагента и Сертификат Уполномоченного лица Банка в виде файла и заверенные распечатки Сертификатов Уполномоченных лиц Банка и Контрагента.

3.5.5. Контрагент заверяет распечатки Сертификатов подписью уполномоченного должностного лица, скрепляет печатью и по одному экземпляру каждой распечатки возвращает в Банк.

3.5.6. Банк регистрирует подписанные Контрагентом распечатки Сертификатов, указывая дату и время регистрации в распечатке Сертификата (Приложение № 2 к настоящему Соглашению)

3.6. После выполнения всех действий по обмену Сертификатами, перечисленных в пункте 3.5. настоящего Соглашения, Криптографические ключи и Сертификаты Уполномоченных лиц Банка и Контрагента считаются действующими и могут использоваться при обмене Электронными документами между Сторонами.

4. ПОРЯДОК ЗАМЕНЫ И ОТЗЫВА СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭП

4.1. Срок действия Сертификата определяется в параметрах Сертификата. Заблаговременно, до истечения срока действия Сертификата Сторона, у которой срок действия Сертификата истекает, должна заново пройти процедуру формирования Криптографических ключей и получения Сертификата в соответствии с п.3.5. и п.3.6. настоящего Соглашения. При вступлении в действие нового Сертификата прежний Сертификат считается отмененным.

4.2. Каждая Сторона может отменить действие Сертификата своего уполномоченного лица, передав другой Стороне письменное уведомление об отмене действия Сертификата (Приложение № 3 к настоящему Соглашению).

4.3. Сертификат Уполномоченного лица Банка или Контрагента считается отмененным с даты отмены действия Сертификата, указанной в уведомлении об отмене действия Сертификата, но не ранее даты получения и регистрации этого уведомления другой Стороной.

5. ПОРЯДОК ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

5.1. Формирование Электронной подписи осуществляется с использованием Ключа электронной подписи Уполномоченного лица отправителя, а проверка Электронной подписи осуществляется с использованием Ключа проверки электронной подписи Уполномоченного лица отправителя.

5.2. Формирование и передача Электронных документов производится Сторонами в следующем порядке:

5.2.1. Электронный документ подписывается Электронной подписью и Шифруется с помощью программного обеспечения СЗИ (используется File-PRO).

5.2.2. Электронный документ отправляется по электронной почте в сети Интернет на адрес принимающей Стороны или, согласно п.2.2., передается принимающей Стороне на съемном носителе информации.

5.3. Стороны принимают и рассматривают Электронные документы при условии, что эти документы были зашифрованы, подписаны электронной подписью Уполномоченных лиц и проверкой Подтверждена подлинность Электронной подписи в электронном документе.

5.4. Ключ проверки электронной подписи Уполномоченного лица Банка или Контрагента считается действующим в момент проверки Электронной подписи при одновременном выполнении следующих условий:

5.4.1. Сертификат зарегистрирован в Банке.

5.4.2. Срок действия Сертификата не истек.

5.4.3. Действие Сертификата не отменено.

5.5. Основаниями для отказа в принятии и рассмотрении Стороной Электронных документов являются следующие:

5.5.1. Электронный документ не зашифрован.

5.5.2. Зашифрованный документ не поддается расшифрованию.

5.5.3. Электронный документ не подписан Электронной подписью.

5.5.4. Проверка не подтвердила подлинности Электронной подписи в электронном документе.

5.5.5. Сертификат ключа проверки электронной подписи прекратил свое действие.

5.6. В случае наличия оснований для отказа от принятия и рассмотрения Электронных документов, перечисленных в пункте 5.5. настоящего Соглашения, обнаружения ошибок в Электронных документах или при возникновении сбоев во время их передачи Стороны незамедлительно уведомляют друг друга о возникших проблемах.

6. ОБЯЗАННОСТИ, ПРАВА И ОТВЕТСТВЕННОСТЬ СТОРОН

6.1. Банк обязан:

6.1.1. Предоставить Контрагенту после заключения настоящего Соглашения во временное пользование программное обеспечение СЗИ и оказать консультативную помощь при его установке и настройке.

6.1.2. Контролировать правильность оформления Электронных документов, предназначенных для обмена с Контрагентом, их надлежащую комплектность, а также следить за соответствием подписываемых электронной подписью документов полномочиям лица, указанного в Сертификате.

6.1.3. Не менее чем за 24 часа извещать Контрагента о планируемых технических изменениях, влияющих на передачу или получение Контрагентом Электронных документов. Если технические изменения приводят к необходимости реконфигурации технических средств или общесистемного программного обеспечения, Банк обязан сообщить об этом Контрагенту не менее чем за 7 календарных дней до даты начала работы в новых условиях.

6.2. Банк имеет право:

6.2.1. Производить замену версий программного обеспечения СЗИ.

6.2.2. Приостановить прием и передачу Электронных документов на время производства плановых технических работ.

6.2.3. В случае выявления признаков нарушения безопасности или подозрения на возможный несанкционированный доступ к передаваемым Электронным документам приостановить прием и передачу Электронных документов.

6.3. Контрагент обязан

6.3.1. Выдать доверенности, уполномоченным сотрудникам Контрагента для обмена Электронными документами с Банком, самостоятельно следить за изменениями полномочий, предоставленных доверенностью, и своевременно информировать Банк об этих изменениях в письменном виде.

6.3.2. Не передавать третьим лицам программное обеспечение, предоставленное Банком в рамках настоящего Соглашения.

6.3.3. Использовать предоставленное Банком программное обеспечение только для целей, определенных настоящим Соглашением.

6.3.4. Производить установку новых версий программного обеспечения, предоставляемых Банком.

6.3.5. По истечении срока действия Соглашения уничтожить все версии программного обеспечения, предоставленного Банком в рамках настоящего Соглашения.

6.4. Стороны обязаны:

6.4.1. Организовать внутренний режим функционирования рабочих мест системы ЭДО таким образом, чтобы исключить возможность доступа к ним посторонних и неуполномоченных лиц.

6.4.2. Обеспечить режим конфиденциальности в отношении передаваемых Электронных документов.

6.4.3. Обеспечить условия для установки и эксплуатации СЗИ в соответствии с требованиями, изложенными в Приложение 1 к Соглашению

6.4.4. Обеспечить условия хранения и использования Криптографических ключей, исключающие их компрометацию.

6.4.5. Сторона, допустившая компрометацию своих Криптографических ключей, независимо от наличия или отсутствия сведений об их несанкционированном использовании, обязана незамедлительно сообщить об этом другой Стороне и прекратить передачу электронных документов до момента регистрации и ввода в действие новых ключей.

6.4.6. Сторона, получившая уведомление о компрометации Криптографических ключей другой Стороны, должна незамедлительно прекратить исполнение электронных документов подписанных ЭП с использованием скомпрометированных ключей.

6.4.7. Обеспечивать сохранение в тайне любой информации, касающейся технологии ЭДО между Сторонами, за исключением случаев, предусмотренных законодательством Российской Федерации.

6.4.8. При выявлении одной из Сторон признаков или фактов нарушения безопасности ЭДО немедленно приостановить ЭДО и известить другую Сторону для принятия совместных мер.

6.4.9. Формировать и поддерживать следующие архивы:

6.4.9.1. Ключи проверки электронной подписи другой Стороны и их Сертификаты, а также оформленные распечатки Сертификатов и Уведомлений об отмене действия Сертификата.

6.4.9.2. Собственные Ключи электронной подписи, ключи проверки и соответствующие им Сертификаты, а также оформленные распечатки Сертификатов и Уведомлений об отмене действия Сертификата.

6.4.9.3. Переданные и принятые электронные документы с установленной ЭП.

6.5. Ответственность Сторон

6.5.1. Стороны несут ответственность за возможные последствия, связанные с нарушением режима конфиденциальности передаваемой информации и, в частности, с передачей Электронных документов в незашифрованном виде.

6.5.2. Стороны не несут ответственности за несвоевременную доставку Электронных документов, связанную с ненадежностью работы сети Интернет или электронной почты.

6.5.3. За неисполнение или ненадлежащее исполнение обязательств по настоящему Соглашению виновная Сторона несет ответственность в соответствии с законодательством Российской Федерации.

7. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

7.1. В случае возникновения обстоятельств непреодолимой силы, то есть чрезвычайных и непредотвратимых при данных условиях обстоятельств, Сторона, пострадавшая от влияния таких обстоятельств непреодолимой силы, освобождается от ответственности за неисполнение, ненадлежащее исполнение обязательств по Соглашению.

7.2. Если обстоятельства, перечисленные в п.7.1. настоящего Соглашения, и их последствия продолжают действовать более 7 (семи) календарных дней, Стороны проводят дополнительные переговоры для выявления приемлемых альтернативных способов исполнения настоящего Соглашения или о досрочном прекращении его действия

8. СРОК ДЕЙСТВИЯ И РАСТОРЖЕНИЕ СОГЛАШЕНИЯ

8.1. Соглашение вступает в силу с даты его подписания Сторонами и действует в течение срока действия Договора.

8.2. Действие настоящего Соглашения ограничено сроком действия Договора.

8.3. Соглашение может быть расторгнуто по требованию любой из Сторон с уведомлением другой Стороны о намерении расторгнуть Соглашение.

8.4. В случае расторжения Соглашения:

8.4.1. По инициативе Банка – Соглашение считается расторгнутым с даты и времени, указанных в уведомлении Банка о расторжении Соглашения.

8.4.2. По инициативе Контрагента – Соглашение считается расторгнутым по истечении часа с момента регистрации в Банке уведомления Контрагента о расторжении Соглашения.

8.5. Расторжение Соглашения не влечет расторжения других договоров (соглашений) между Сторонами в части, не касающейся передачи Электронных документов, в рамках Соглашения.

9. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

9.1. Все споры и разногласия, возникающие из настоящего Соглашения или в связи с ним разрешаются Сторонами путем переговоров.

9.2. При возникновении спорных ситуаций, связанных с исполнением или неисполнением Электронного документа, подписанного Электронной подписью, Стороны осуществляют

действия, определенные разделом 10 настоящего Соглашения.

9.3. В случае если Стороны не придут к соглашению, споры и разногласия подлежат разрешению в Арбитражном суде г. Москвы в соответствии с законодательством Российской Федерации.

10. ПОРЯДОК РАЗРЕШЕНИЯ СПОРНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ИСПОЛНЕНИЕМ ИЛИ НЕИСПОЛНЕНИЕМ ЭЛЕКТРОННОГО ДОКУМЕНТА, ПОДПИСАННОГО ЭП

10.1. При возникновении между Сторонами споров и разногласий, связанных с исполнением или неисполнением Электронного документа, подписанного Электронной подписью, Стороны создают комиссию для претензионного урегулирования спорной ситуации. Комиссия создается по инициативе одной из Сторон в течение четырнадцати календарных дней с даты уведомления официальным письмом инициирующей создание данной комиссии стороной вторую сторону о необходимости претензионного урегулирования спорной ситуации.

10.2. В состав комиссии должно входить равное количество представителей от каждой из Сторон. При необходимости с письменного согласия обеих Сторон в состав комиссии могут быть дополнительно введены эксперты третьей стороны. Состав комиссии должен быть зафиксирован в Акте, который является итоговым документом, отражающим результаты работы комиссии. Полномочия членов комиссии подтверждаются доверенностями, выданными в установленном порядке. Срок работы комиссии составляет не более пяти рабочих дней. При необходимости этот срок может быть увеличен до одного месяца.

10.3. Стороны способствуют работе комиссии и не допускают отказа от предоставления необходимых документов.

10.4. Комиссия определяет корректность или некорректность Электронной подписи спорного Электронного документа с помощью процедуры технической экспертизы, которая проводится в соответствии с нижеследующим порядком:

10.4.1. Комиссия получает в ЗАО «Сигнал-КОМ» и устанавливает эталонную версию программного обеспечения «File-Pro».

10.4.2. Стороны предъявляют комиссии:

- свою электронную архивную копию спорного Электронного документа с Электронной подписью;
- свою электронную архивную копию Сертификата, предназначенного для проверки Электронной подписи спорного Электронного документа;
- свою архивную копию распечатки Сертификата, заверенную обеими Сторонами;
- свой экземпляр Заявления об отмене действия Сертификата (при наличии);

В случае непредъявления комиссии одной из Сторон какого-либо из вышеперечисленных документов к рассмотрению принимается экземпляр указанного документа, представленный другой Стороной.

10.4.3. Комиссия устанавливает идентичность значений электронной архивной копии Сертификата, с помощью которого проверялась Электронная подпись спорного Электронного документа, архивной копии распечатки этого Сертификата. В случае неидентичности хотя бы одного из значений сравниваемых Сертификатов Электронная подпись спорного Электронного документа признается некорректной и процедура технической экспертизы считается завершенной.

10.4.4. В случае наличия Заявления об отмене действия Сертификата, предназначенного для проверки Электронной подписи спорного Электронного документа, комиссия устанавливает идентичность значений серийного номера Сертификата, которые содержатся в электронной архивной копии Сертификата и в архивной копии Заявления об отмене действия

Сертификата, а также дату отмены Сертификата и дату регистрации Заявления. В случае идентичности указанных значений серийного номера Сертификата и если Электронный документ подписан Электронной подписью позже даты отмены Сертификата и даты регистрации Заявления об отмене Сертификата, Электронная подпись спорного Электронного документа признается некорректной и процедура технической экспертизы считается завершённой.

10.4.5. Комиссия с помощью эталонной версии программного обеспечения «File-PRO» производит проверку Электронной подписи архивной копии спорного Электронного документа с использованием электронной архивной копии Сертификата. После установления комиссией корректности или некорректности Электронной подписи спорного Электронного документа процедура технической экспертизы считается завершённой.

10.5. В том случае, если Банк принял к исполнению полученный от Контрагента оспариваемый Электронный документ, подписанный Электронной подписью, некорректность которой установлена комиссией, претензии Контрагента к Банку, связанные с последствиями исполнения указанного оспариваемого Электронного документа, признаются комиссией обоснованными.

10.6. В том случае, если Контрагент приняло к исполнению полученный от Банка оспариваемый Электронный документ, подписанный Электронной подписью, некорректность которой установлена комиссией, претензии Банка к Контрагенту, связанные с последствиями исполнения указанного оспариваемого Электронного документа, признаются комиссией обоснованными.

10.7. В случае возникновения спорной ситуации, связанной с отказом Банка от факта получения Электронного документа, комиссия определяет корректность или некорректность Электронной подписи квитанции, представленной Контрагентом, в соответствии с процедурой, описанной в п. 10.4 настоящего Соглашения.

10.8. В случае подтверждения корректности Электронной подписи квитанции, представленной Контрагентом, претензии Контрагента Банку, связанные с последствиями отказа Банка от факта получения Электронного документа, признаются комиссией обоснованными.

10.9. По итогам работы комиссии составляется Акт, в котором в обязательном порядке отражаются:

- установленные обстоятельства;
- действия членов комиссии;
- выводы комиссии;
- основания для формирования выводов.

10.10. Составленный комиссией Акт утверждается Сторонами и является основанием для принятия Сторонами окончательного решения в рамках претензионного урегулирования спорной ситуации.

10.11. В случае если Стороны в рамках претензионного урегулирования спорной ситуации пришли к взаимоприемлемому соглашению, то они в течение четырнадцати календарных дней с даты окончания работы комиссии составляют соответствующий двусторонний Акт, условия которого являются обязательными для выполнения каждой из Сторон.

10.12. В случае если Стороны в рамках претензионного урегулирования спорной ситуации не пришли к взаимоприемлемому соглашению, то заинтересованная Сторона вправе обратиться в Арбитражный суд и в качестве доказательства в судебном споре обязана представить Акт, составленный в соответствии с настоящим Порядком. Представленный в Арбитражный суд Акт имеет равную силу с другими доказательствами, представленными Сторонами.

11. ПРОЧИЕ УСЛОВИЯ

11.1. Настоящее Соглашение составлено в двух экземплярах, по одному для каждой из Сторон. Оба экземпляра идентичны и имеют одинаковую юридическую силу

11.2. Изменения и дополнения к настоящему Соглашению считаются действительными, если они совершены в письменном виде и подписаны Сторонами.

11.3. Все Приложения к настоящему Соглашению являются его неотъемлемой частью и имеют равную с ним юридическую силу.

11.4. В случае изменения юридического, почтового адреса и банковских реквизитов Стороны обязаны незамедлительно уведомить об этом друг друга.

11.5. Соглашение имеет следующие приложения, являющиеся его неотъемлемой частью:

11.5.1. Приложение № 1– требования по обеспечению информационной безопасности при организации защищенного электронного документооборота.

11.5.2. Приложение № 2– Сертификат ключа проверки электронной подписи.

11.5.3. Приложение № 3 – Уведомление об отмене действия Сертификата ключа проверки электронной подписи.

12. ЮРИДИЧЕСКИЕ АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН

Банк:

ВТБ (ПАО)
Адрес местонахождения:
Юр. адрес: 190000, г. Санкт-Петербург, ул. Большая Морская, д 29
Филиал № 7701 Банка ВТБ (ПАО) в г. Москве
Юр. адрес: 101000, г. Москва, ул. Мясницкая, д. 35
Почт. адрес: 109147, г. Москва, ул. Воронцовская, д.43, стр.1
Банковские реквизиты:
БИК 044525745, ИНН 7702070139, КПП 770943003
к/с 30101810345250000745 в Отделении 1 Москва ГУ Банка России по ЦФО

Контрагент:

ООО ВТБ Капитал Пенсионный резерв
Юр. адрес: 123112, г. Москва, наб. Пресненская, д.10, этаж 15, помещение III, комната 20
Почт. адрес: 123112, г. Москва, наб. Пресненская, д.10, этаж 15, помещение III, комната 20
e-mail: BSSIM_OPIF@vtbcapital.com
Банковские реквизиты:
БИК 044525187, ИНН 7722270922, КПП 770301001
Р/с: 40701810600030000279 в Банк ВТБ (ПАО) г. Москва,
К/с 30101 810 7 0000 0000 187

13. ПОДПИСИ СТОРОН

За Банк: _____ **/ Потапов В.М./**

м.п.

За Контрагента: _____ **/ Волгин О.Н./**

м.п.

Приложение № 1
к Соглашению от

ТРЕБОВАНИЯ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ ЗАЩИЩИЩЕННОГО ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

1. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ СЗИ

1.1. Автоматизированные рабочие места с СЗИ должны располагаться в помещениях, обеспечивающих невозможность несанкционированного доступа к СЗИ.

1.2. Правом доступа к рабочим местам с СЗИ должны обладать только лица, ознакомленные с правилами пользования СЗИ и с другими нормативными документами, созданными на их основе.

1.3. Запрещается оставлять без контроля вычислительные средства, на которых установлены СЗИ, при включенном питании и загруженном программном обеспечении. При кратковременном перерыве в работе рекомендуется производить гашение экрана, возобновление активности экрана должно производиться с использованием пароля доступа.

1.4. На компьютере с установленным СЗИ должны запускаться только те приложения, которые разрешены администратором.

1.5. На компьютере должна быть установлена только одна операционная система.

1.6. На компьютере должна быть установлена парольная защита на вход в BIOS и в операционную систему. Пароль должен обладать необходимой сложностью, исключающей его подбор по словарю. Рекомендуемые параметры: длина не менее 6 символов, включая 3 из 4 возможных групп символов: строчные буквы, прописные буквы, цифры и спецсимволы (!»;%:?* и пр.).

1.7. При использовании СЗИ на компьютере, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СЗИ, и к компонентам СЗИ со стороны указанных сетей.

1.8. Управление привилегиями, квотами и установке прав доступа пользователей к файловой системе должен осуществлять только администратор системы по согласованию со службой информационной безопасности.

1.9. Рабочие места должны быть защищены с помощью специальных программных и аппаратных средств антивирусной защиты (сетевых или персональных).

1.10. Программное обеспечение, установленное на компьютере, не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.

1.11. Не следует исполнять и открывать файлы, полученные из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов.

2. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ХРАНЕНИИ И ИСПОЛЬЗОВАНИИ КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ.

2.1. Автоматизированные рабочие места, на которых осуществляется работа с криптографическими ключами, должны использоваться в соответствии с эксплуатационной документацией и только в рамках электронного документооборота.

2.2. Доступ неуполномоченных лиц к носителям ключевой информации должен быть исключен.

2.3. Не допускается:

2.3.1. Снимать копии с носителей ключевой информации.

2.3.2. Знакомить с содержанием носителей ключевой информации или передавать носители ключевой информации лицам, к ним не допущенным.

2.3.3. Выводить криптографические ключи на дисплей (монитор) электронно-вычислительной машины (ЭВМ) или принтер.

2.3.4. Устанавливать ключевой носитель в считывающее устройство АРМ, программные средства которого функционируют в непредусмотренных (нештатных) режимах, а также на другие ЭВМ.

2.3.5. Записывать на носители ключевой информации постороннюю информацию.

2.3.6. Передавать криптографические ключи по линиям связи в открытом виде.

2.4. В случае компрометации криптографических ключей должна быть проведена их замена.

За Банк:

/ Потапов В.М./

м.п.

За Контрагента:

/ Волгин О.Н./

м.п.

Приложение № 2

к Соглашению от

Сертификат ключа проверки электронной подписи.

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            01:4e:03:09:f5:4c:01:0b:03:09:7e:6e
        Signature Algorithm: ecr3410WithR3411 (1.3.6.1.4.1.5849.1.3.2)
        Issuer: C=RU, L=МОСКВА, O=ВТБ (ПАО), CN=Удостоверяющий Центр, Email=cacenter@vtb24.ru
        Validity
            Not Before: Jul  9 12:21:12 2013 GMT
            Not After : Jul  9 12:21:12 2015 GMT
        Subject: C=RU, L=Москва, O="ООО "РОМАШКА"", OU=Отдел продаж, T=Начальник отдела, CN=Чапаев Петр Васильевич,
Email=Chapaev_PV@romashka.ru
        Subject Public Key Info:
            Public Key Algorithm: ecr3410 (1.3.6.1.4.1.5849.1.6.2)
            ECGOST Public Key:
                pub:
                    04:a5:f8:7c:57:70:fa:80:e6:73:bc:2c:0c:7a:31:
                    04:4b:80:9f:5f:c7:a0:f3:e1:c0:53:5e:49:89:17:
                    aa:c4:ff:6f:c8:34:1d:04:bc:14:19:8e:84:91:e1:
                    80:53:47:d9:fa:b7:9f:6c:29:93:10:dc:bc:a1:52:
                    09:d3:07:15:22
                prime:  (256 bits)
                    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
                    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
                    ff:ff:ff
                a:  (256 bits)
                    00:ff:ff:ff:ff:00:00:00:01:00:00:00:00:00:00:
                    00:00:00:00:00:00:ff:ff:ff:ff:ff:ff:ff:ff:ff:
                    ff:ff:fc
                b:  (255 bits)
                    5a:c6:35:d8:aa:3a:93:e7:b3:eb:bd:55:76:98:86:
                    bc:65:1d:06:b0:cc:53:b0:f6:3b:ce:3c:3e:27:d2:
                    60:4b
                base:
                    04:6b:17:d1:f2:e1:2c:42:47:f8:bc:e6:e5:63:a4:
                    40:f2:77:03:7d:81:2d:eb:33:a0:f4:a1:39:45:d8:
                    98:c2:96:4f:e3:42:e2:fe:1a:7f:9b:8e:e7:eb:4a:
                    7c:0f:9e:16:2b:ce:33:57:6b:31:5e:ce:cb:b6:40:
                    68:37:bf:51:f5
                order:  (256 bits)
                    00:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:ff:
                    ff:ff:bc:e6:fa:ad:a7:17:9e:84:f3:b9:ca:c2:fc:
                    63:25:51
                cofactor:  (1 bit)
                    01
    Signature Algorithm: ecr3410WithR3411 (1.3.6.1.4.1.5849.1.3.2)
        30:44:02:20:7e:0c:65:39:aa:cb:34:07:fd:35:7c:cc:50:58:
        b4:98:e5:ac:5d:6d:db:fa:41:ba:5b:8a:5f:3e:22:76:61:59:
        02:20:16:8f:e1:49:89:fc:35:72:f6:ef:49:4c:c6:5b:3e:c2:
        01:60:32:35:7d:f8:1f:e2:16:50:ca:f0:36:76:cf:6e
```

Подпись владельца сертификата ключа проверки ЭП: _____

Сертификат зарегистрирован в Банке «____»_____20__г. ___час. ___мин.

_____

(Должность, ФИО, подпись сотрудника Банка)

Сертификат действует с момента регистрации в Банке.

За Банк:

_____ **/ Потапов В.М./**

М.П.

За Контрагента:

_____ **/ Волгин О.Н./**

М.П.

Типовая форма № 55Х-355/201
Приложение № 3
к Соглашению от

Уведомление

об отмене действия Сертификата ключа проверки электронной подписи

_____просит с «___» _____ 20__г. отменить действие Сертификата ключа
(наименование Контрагента)
проверки электронной подписи уполномоченного лица _____
(Ф.И.О.)

Serial Number _____.
(*Serial Number Сертификата*)

_____ _____ _____
(Руководитель) *(подпись)* *(Ф.И.О.)*
«____» _____ 20 __ г.

М.П.

Уведомление зарегистрировано в Банке «____»_____20 __г. ___ час. ____мин.

_____ _____
(подпись) *(Ф.И.О.)*

М.П.

Всего прошито, пронумеровано и
скреплено печатью 14 (четырнадцать) лист/а/ов.
Генеральный директор
ООО ВТБ Капитал Пенсионный резерв

_____ Волгин О.Н.