УТВЕРЖДЕНЫ
Приказом Генерального директора
ООО «ДОХОДНЫЙ ДОМ ИНВЕСТОРА»
№ 28 от 21 ноября 2014 г.

ПРАВИЛА ОБМЕНА ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ ООО “ДОХОДНЫЙ ДОМ ИНВЕСТОРА”

1. Термины и определения

Система обмена электронными документами (СОЭД) – корпоративная информационная система, представляющая собой совокупность программного и аппаратного обеспечения, в рамках которой происходит передача (обмен) информации в электронной форме между её участниками - ООО “ДОХОДНЫЙ ДОМ ИНВЕСТОРА (далее - “ОПЕРАТОР”), с одной стороны, и его клиентами (юридическими и физическими лицами), с другой;

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, подписанная электронной подписью участника СОЭД;

Электронная подпись — 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;

Средства электронной подписи (СЭП) – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

СЭП могут применяться как в виде самостоятельных программных модулей, так и в виде инструментальных средств, встраиваемых в прикладное программное обеспечение.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Сертификат ключа проверки электронной подписи (Сертификат) – электронный документ или документ на бумажном носителе, выданные ОПЕРАТОРОМ Клиенту и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи;

Владелец Сертификата ключа проверки электронной подписи — лицо, которому ОПЕРАТОРОМ выдан Сертификат ключа проверки электронной подписи.

Компрометация ключа электронной подписи (компрометация ключа) – констатация владельцем ключа электронной подписи обстоятельств или наступления обстоятельств, при которых возможно несанкционированное использование ключа электронной подписи неуполномоченными лицами.

Подтверждение подлинности электронной цифровой подписи в электронном документе — положительный результат проверки электронной подписи принадлежности электронной подписи в электронном документе владельцу Сертификата ключа электронной подписи и отсутствия искажений в подписанном данной электронной подписью электронном документе.

Отправитель - участник СОЭД, направивший электронный документ другому участнику СОЭД.

Получатель - участник СОЭД, которому другим участником СОЭД был отправлен электронный документ.

2. Общие положения

2.1. Электронный документ, подписанный электронной подписью, признаётся равнозначным документу на бумажном носителе, подписанному собственноручной подписью.

2.2. Одной электронной подписью могут быть подписаны несколько связанных между собой документов (пакет электронных документов). При этом каждый из электронных документов, входящих в этот пакет, считается подписанным электронной подписью.

2.2. Клиент считается участником СОЭД после:

2.2.1. заключения с ОПЕРАТОРОМ соглашения об использовании электронной подписи;

2.2.2. проведения мероприятий по наладке (установке) на имеющемся у него персональном компьютере или ином электронном устройстве программного обеспечения, необходимого для обмена с ОПЕРАТОРОМ электронными документами в соответствии с настоящими Правилами;

2.2.3. создания ключа электронной подписи;

2.2.4. проверки и активации ОПЕРАТОРОМ ключа электронной подписи.

3. Требования, предъявляемые к электронному документу

3.1. Электронный документ имеет юридическую силу, если сформирован в формате, предусмотренном СОЭД, подписан электронной подписью и получен положительный результат проверки электронной подписи этого электронного документа.

3.3. Электронный документ без электронной подписи или, имеющий формат, который не применяется в СОЭД, считается не полученным.

3.1. Для подписания электронного документа участники СОЭД используют неквалифицированную электронную подпись, которая:

- получена в результате криптографического преобразования информации с использованием ключа электронной подписи;
- позволяет определить лицо, подписавшее электронный документ;
- позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;
- создаётся с использованием средств электронной подписи.

3.4. Ответственность за неправомерное использования электронной подписи несёт участник СОЭД, на имя которого зарегистрирован Сертификат ключа проверки электронной подписи.

3.5. Электронный документ признается полученным Получателем с момента получения Отправителем от Получателя подтверждения о получении электронного документа.

4. Права и обязанности Участников СОЭД

4.4. Участники СОЭД обязаны:

4.4.1. обеспечить конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

4.4.2. немедленно уведомлять друг друга, используя любые виды связи, о нарушении конфиденциальности принадлежащий им ключей электронных подписей и в письменной форме - в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

4.4.3. не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

4.4.4. принимать меры по предотвращению раскрытия и/или воспроизведения (распространения) любой информации, связанной с работой СОЭД, а также любой иной информации, которая становится ему доступной в связи с работой в СОЭД;

4.4.5. определить лицо, имеющее право подписывать электронной подписью электронные документы, и уведомить об этом контрагента.

4.5. Клиент обязан:

4.5.1. предоставить ОПЕРАТОРУ достоверные сведения о себе, необходимые для осуществления взаимодействия в СОЭД в порядке, предусмотренном законодательством, нормативными правовыми актами и настоящими Правилами;

4.5.2. за 10 (Десять) календарных дней до окончания срока действия Сертификата ключа проверки электронной подписи принять меры по получению нового Сертификата.

4.5.3. предоставить ОПЕРАТОРУ доверенность на подписание электронных документов в СЭД на своего уполномоченного представителя – владельца сертификата ключа проверки электронной подписи, в которой Клиент должен определить полномочия владельца сертификата проверки электронной подписи на подписание электронных документов в СОЭД. Предоставление указанной доверенности не требуется в случае, если уполномоченный представитель Клиента – владелец сертификата ключа проверки электронной подписи действует от имени Клиента на основании закона и/или учредительных документов Клиента, или у ОПЕРАТОРА имеется доверенность Клиента на данного уполномоченного представителя (и по данному депозитарному коду), срок действия которой не истёк.

4.5.4. Владелец ключа электронной подписи обязан хранить его в электронном виде, в том числе и по истечении срока действия Сертификата, не менее трёх лет.

5. Организация электронного документооборота

5.1. Электронный документооборот включает:

- формирование электронного документа (включая его подписание электронной подписью);
- отправку электронного документа;
- проверку электронного документа;
- подтверждение получения электронного документа;
- учёт электронного документа (регистрацию входящих и исходящих электронных документов);
- хранение электронных документов (ведение архива электронных документов).

5.2. Электронный документ считается исходящим от Отправителя, если электронный документ отправлен Отправителем или от имени Отправителя - автоматическим процессом, который представляет собой часть программного и аппаратного обеспечения СОЭД.

5.3. Электронный документ не считается исходящим от Отправителя, если Получатель электронного документа знал или должен был знать, в том числе в результате выполнения проверки, о том, что электронный документ не исходит от Отправителя, или Получатель знал или должен был знать, в том числе в результате выполнения проверки электронной подписи, о том, что получен искаженный электронный документ.

5.4. Проверка электронного документа включает его расшифровку, подтверждение подлинности электронной подписи в электронном документе и отсутствие изменений, внесённых в этот документ после его подписания.

5.5. В случае положительного результата проверки электронного документа, данный электронный документ принимается к исполнению или подлежит дальнейшей обработке. В противном случае данный электронный документ считается не полученным, о чём Получатель должен направить Отправителю уведомление с указанием причины неполучения документа.

5.6. Учёт электронных документов осуществляется посредством электронных журналов учёта. Программные средства ведения электронных журналов учёта электронных документов являются составной частью программного обеспечения СЭД.

5.7. Для выполнения работ по учёту электронных документов Участниками должны быть назначено ответственное лицо (лица).

5.8. При учёте исходящего электронного документа Отправитель должен обеспечить учёт следующих данных:

- уникальный исходящий номер электронного документа;
- дату и время создания электронного документа, дату и время подписания электронного документа электронной подписью;
- отметку об отправке электронного документа;
- иные данные по усмотрению Отправителя.

5.9. При учёте входящего электронного документа Получатель должен обеспечить учёт следующих данных:

- уникальный входящий номер электронного документа;
- дату и время получения электронного документа;
- исходящий номер полученного электронного документа,

5.10. ОПЕРАТОР обязан обеспечить защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учётных данных, содержащихся в электронном журнале учёта электронных документов. Срок хранения учётных данных не может быть менее трёх лет.

5.11. Все электронные документы, учтенные в СЭД, должны храниться в течение сроков, предусмотренных внутренними документами ОПЕРАТОРА. Электронные документы должны храниться в электронном архиве.

5.12. Электронные документы должны храниться в том же формате, в котором они были сформированы, отправлены и/или получены.

5.13. Хранение электронных документов производиться с Сертификатами ключей проверки электронной подписи и с соответствующим программным обеспечением, обеспечивающего возможность работы с электронными документами и проверки электронной подписи электронных документов.

5.14. Обязанности хранения электронных документов возлагаются на участников СОЭД.

5.15. Для ведения электронного архива участниками СОЭД должны быть назначены ответственные лица, имеющие необходимое для выполнения этих функций образование и/или опыт (навыки) работы.

6. Система обеспечения информационной безопасности

6.1. Участники СОЭД должны принимать все зависящие от них меры, необходимые для защиты информации содержащейся в электронных документах, обмен которыми производится в СОЭД.

6.2. Соблюдение требований информационной безопасности при организации электронного документооборота обеспечивает:

- конфиденциальность информации (получить доступ к информации могут только уполномоченные лица);
- целостность передаваемой информации (гарантирование, что данные передаются без искажений, и исключается возможность подмены информации);
- аутентификацию (когда передаваемую информацию может получить только то лицо, кому она предназначена, а отправителем является именно тот, от чьего имени она отправлена).

6.3. Требования по информационной безопасности при осуществлении обмена электронными документами реализуются посредством применения программно-технических средств и организационных мер в СОЭД.

6.4. К программно-техническим средствам относятся:

- программные средства, специально разработанные для осуществления электронного документооборота;
- система паролей и идентификаторов для ограничения доступа к программному и аппаратному обеспечению, а также к техническим средствам СОЭД;
- средства электронной подписи;
- средства криптографической защиты информации;
- программно-аппаратные средства защиты от несанкционированного доступа в СОЭД;
- средства защиты от программных вирусов;

6.5. К организационным мерам относятся:

- размещение технических средств обеспечивающих функционирование СОЭ в помещениях ОПЕРАТОРА с контролируемым доступом к ним;
- административные ограничения доступа к этим средствам;
- задание режима использования паролей и идентификаторов.

7. Заключительные положения

7.1. Настоящие Правила разработаны в соответствии с Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи».

7.2. В случаях, не предусмотренных настоящими Правилами, участники СОЭД руководствуются федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, регулирующими отношения в области обмена электронными документами, в том числе с использованием электронной подписи.