УТВЕРЖДАЮ

Генеральный директор
ОАО «ИнфоТеКС Интернет Траст»

А.Е. Прошин

"07" июня 2018 г.

РЕГЛАМЕНТ
информационной системы "IITrustCloud"

(версия 2.5)

г. Москва
2018 г.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Администратор Документооборота – Участник Системы (юридическое лицо или индивидуальный предприниматель), наделенный Оператором полномочиями по определению состава и параметров Документооборота, а также состава участников Документооборота из числа иных Участников Системы.

Владелец сертификата ключа проверки электронной подписи – лицо, которому в установленном федеральным законодательством порядке выдан сертификат ключа проверки электронной подписи.

Доверенный сервис электронной подписи – технологическое решение на базе программно-аппаратного комплекса ViPNet Hardware Secure Module (ViPNet HSM), реализованное в рамках информационной системы "IITrustCloud", обеспечивающее централизованное безопасное хранение ключей и сертификатов ключей проверки электронных подписей Участников Системы, а также удаленное выполнение операций по созданию и проверке усиленных неквалифицированных электронных подписей в интересах Участников Системы.

Документооборот – совокупность взаимосвязанных процедур, обеспечивающих движение документов определенного состава между Участниками Системы в соответствии с параметрами, определенными Администратором Документооборота, с момента создания или поступления документов и до завершения выполнения с документами всех необходимых действий.

Информационная система "IITrustCloud" (далее – Система) – корпоративная информационная система, действующая по правилам, установленным Оператором Системы, и обеспечивающая:
- электронный Документооборот между Участниками Системы с использованием усиленных неквалифицированных электронных подписей;
- доступ Участников Системы к Доверенному сервису электронной подписи;
- хранение электронных документов, подписанных усиленными неквалифицированными электронными подписями сторон, и предоставление этих документов любой из сторон данного Документооборота по соответствующему запросу.

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

Ключ простой электронной подписи – сочетание двух элементов - идентификатора и пароля ключа.

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

Личный кабинет – персональное информационное пространство Участника Системы, формируемое в Системе при регистрации Участника.

Неквалифицированный сертификат – сертификат ключа проверки усиленной неквалифицированной электронной подписи.

Оператор информационной системы "IITrustCloud" (далее – Оператор) – открытое акционерное общество «ИнфоТеКС Интернет Траст», которое обладает законными правами на Систему и устанавливает порядок информационного взаимодействия между участниками Системы.

Параметры Документооборота – набор настраиваемых свойств Документооборота, определяемых Администратором Документооборота, включая:
- количество подписантов документов;
- способ оповещения о направлении документа на подпись;

- тип документа (формализованный или неформализованный);
- способ ознакомления подписанта с подписываемым документом;
- способ подтверждения согласия на подписание документа;
- полномочия Представителей Администратора Документооборота.

Представитель Администратора Документооборота – Участник Системы (юридическое лицо или индивидуальный предприниматель), наделенное Администратором Документооборота правом осуществлять в Системе действия от имени Администратора Документооборота, связанные с регистрацией Пользователей в Системе и осуществлением Документооборота по правилам, установленным Администратором документооборота.

Простая электронная подпись – электронная подпись, которая посредством использования ключа простой электронной подписи подтверждает факт формирования электронной подписи конкретным лицом.

Режим видимости Участников – настройка Системы, отвечающая за допущение (открытый режим видимости Участников) или не допущение (закрытый режим видимости Участников) возможности проведения Администратором Документооборота верификации регистрационных данных Участников, зарегистрированных другим Администратором Документооборота и верификации другим Администратором Документооборота регистрационных данных Участников, зарегистрированных Администратором Документооборота.

Сертификат ключа проверки электронной подписи (далее – сертификат) – электронный документ, выданный Удостоверяющим центром и подтверждающий принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Удостоверяющий центр – ОАО «ИнфоТеКС Интернет Траст», осуществляющее функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом "Об электронной подписи".

Уполномоченный сотрудник – сотрудник юридического лица, наделенный юридическим лицом правом осуществлять в Системе действия от имени юридического лица.

Усиленная неквалифицированная электронная подпись – электронная 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;
- создается с использованием средств электронной подписи.

Участники информационного взаимодействия (далее – Участники Системы, Участники) – зарегистрированные в Системе юридические и физические лица, в том числе индивидуальные предприниматели, присоединившиеся к настоящему Регламенту в порядке, предусмотренном Регламентом.

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.

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.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Настоящий Регламент устанавливает порядок взаимодействия Участников Системы и подписания электронных документов электронной подписью, а также определяет правовые условия, при соблюдении которых электронные документы, подписанные электронной подписью, признаются равнозначным документам на бумажном носителе, подписанным собственноручной подписью.

2.2. Оператором Системы является открытое акционерное общество «ИнфоТеКС Интернет Траст».

2.3. Настоящий Регламент опубликован на сайте Оператора Системы в сети Интернет по адресу https://iitrust.cloud/.

2.4. Настоящий Регламент со всеми Приложениями к нему является договором присоединения в соответствии со ст. 428 Гражданского кодекса РФ.

2.5. Присоединение к настоящему Регламенту осуществляется путем подписания заявителем заявления о присоединении к Регламенту. С момента подписания заявления заявитель считается присоединившимся к Регламенту и становится стороной Регламента (Участником Системы).

2.6. Факт присоединения заявителя к Регламенту является полным принятием им условий настоящего Регламента и всех его приложений в редакции, действующей на момент подписания заявления. Сторона, присоединившаяся к Регламенту, принимает дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями настоящего Регламента.

2.7. Стороны понимают термины, применяемые в настоящем Регламенте, строго в контексте общего смысла Регламента.

3. ЭЛЕКТРОННАЯ ПОДПИСЬ

3.1. Для подписания электронных документов в Системе используются усиленные неквалифицированные электронные подписи, созданные при помощи Доверенного сервиса электронной подписи на основе неквалифицированных сертификатов ключей проверки электронных подписей, выданных Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст».

3.2. Участники Системы соглашаются с тем, что обращающиеся в Системе электронные документы, подписанные усиленной неквалифицированной электронной подписью, признаются электронными документами, равнозначными документам на бумажном носителе, подписанным собственноручной подписью владельца неквалифицированного сертификата ключа проверки электронной подписи.

4. ПОРЯДОК ПРОВЕРКИ УСИЛЕННОЙ НЕКВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

4.1. Проверка усиленной электронной подписи в Системе осуществляется при помощи Доверенного сервиса электронной подписи.

4.2. Неквалифицированная электронная подпись признается действительной при одновременном соблюдении следующих условий:

- сертификат ключа проверки электронной подписи выдан Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст»;

- сертификат является действительным на момент проверки электронной подписи или являлся действительным на момент создания электронной подписи, зафиксированный в Системе;

- результат проверки принадлежности электронной подписи владельцу сертификата – положительный;

- отсутствуют искажения в подписанном данной неквалифицированной электронной подписью электронном документе.

5. УДОСТОВЕРЯЮЩИЙ ЦЕНТР И СЕРТИФИКАТЫ

5.1. Создание неквалифицированных сертификатов для Участников Системы осуществляется в соответствии с Регламентом предоставления Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки электронных подписей, не являющихся квалифицированными, опубликованном на сайте Удостоверяющего центра https://iitrust.ru/.

5.2. Неквалифицированный сертификат ключа проверки электронной подписи, создаваемый Удостоверяющим центром для использования в Системе, должен содержать следующую информацию:
- уникальный номер неквалифицированного сертификата;
- даты начала и окончания действия неквалифицированного сертификата;
- фамилия, имя и отчество (если имеется) физического лица, указанного в качестве владельца неквалифицированного сертификата, в том числе, действующего от имени юридического лица;
- уникальный идентификатор физического лица, указанного в качестве единоличного владельца неквалифицированного сертификата, присваиваемый ему системой «IITrustCloud» на этапе регистрации в Удостоверяющем центре;
- основной государственный регистрационный номер индивидуального предпринимателя (ОГРНИП), указанного в качестве владельца неквалифицированного сертификата;
- наименование и место нахождения юридического лица, указанного в качестве владельца неквалифицированного сертификата;
- основной государственный регистрационный номер (ОГРН) юридического лица, указанного в качестве владельца неквалифицированного сертификата;
- идентификационный номер налогоплательщика (ИНН) юридического лица, указанного в качестве владельца неквалифицированного сертификата;
- ключ проверки электронной подписи.

5.3. Срок действия ключей электронной подписи и неквалифицированного сертификата ключа проверки электронной подписи, создаваемых Удостоверяющим центром для использования в Системе, составляет 36 месяцев.

5.4. Стороны Регламента признают, что информация, содержащаяся в сертификате, однозначно определяет владельца сертификата и соответствующего ключа электронной подписи.

6. ПОРЯДОК РЕГИСТРАЦИИ УЧАСТНИКОВ

6.1. Обязательным условием регистрации Участника в Системе, является наличие у него неквалифицированного сертификата ключа проверки электронной подписи, выданного Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст».

6.2. Регистрация в Системе Участника, не являющегося Администратором Документооборота или Представителем Администратора Документооборота, осуществляется на основании заявления о присоединении к Регламенту Системы, подаваемому заявителем Оператору через Администратора Документооборота или его Представителя в виде документа на бумажном носителе.

6.3. Заявление о присоединении к Регламенту Системы, подаваемое физическим лицом, должно быть подписано собственноручной подписью физического лица и должно содержать следующие сведения:
- фамилия, имя и отчество (если имеется);
- серия и номер паспорта гражданина РФ;

- дата выдачи паспорта гражданина РФ;
- наименование органа, выдавшего паспорт гражданина РФ;
- номер мобильного телефона;
- основной государственный регистрационный номер индивидуального предпринимателя, в случае если физическое лицо регистрируется в Системе в качестве индивидуального предпринимателя.

6.4. Заявление о присоединении к Регламенту Системы, подаваемое юридическим лицом, должно быть подписано собственноручной подписью лица, имеющего право действовать от имени юридического лица на основании учредительных документов юридического лица, и должно содержать следующие сведения:
- наименование юридического лица;
- основной государственный регистрационный номер юридического лица;
- идентификационный номер налогоплательщика - юридического лица;
- сведения о документе, подтверждающем право лица, подписывающего заявление, действовать от имени юридического лица;
- фамилия, имя и отчество (если имеется) Уполномоченного сотрудника юридического лица;
- серия и номер паспорта гражданина РФ Уполномоченного сотрудника юридического лица;
- дата выдачи паспорта гражданина РФ Уполномоченного сотрудника юридического лица;
- наименование органа, выдавшего паспорт гражданина РФ Уполномоченного сотрудника юридического лица;
- номер мобильного телефона Уполномоченного сотрудника юридического лица.

6.5. Регистрация в Системе Участника, являющегося Администратором Документооборота, осуществляется на основании договора об оказании услуг, заключенного между Оператором и Администратором Документооборота. Порядок подключения к Системе Участника, являющегося Администратором Документооборота, определяется на этапе технической реализации взаимодействия Администратора Документооборота с Системой.

6.6. Наделение Участника Системы полномочиями Представителя Администратора Документооборота осуществляется Администратором Документооборота.

6.7. Регистрация в Системе Участника, являющегося Представителем Администратора Документооборота, осуществляется на основании подаваемого Администратором Документооборота Оператору заявления в электронном виде с регистрационными данными Представителя Администратора Документооборота.

6.8. В процессе регистрации в Системе нового Участника ему создается Личный кабинет, для доступа к которому формируется ключ простой электронной подписи.

6.9. Порядок передачи ключа простой электронной подписи для доступа к Личному кабинету Участника, являющегося Администратором Документооборота или Представителем Администратора Документооборота, определяется на этапе технической реализации взаимодействия Администратора Документооборота с Системой.

6.10. Передача ключа простой электронной подписи для доступа к Личному кабинету Участнику Системы, не являющемуся Администратором Документооборота или его Представителем, осуществляется Оператором в составе SMS-сообщения, направляемого на указанный Участником Системы при регистрации номер мобильного телефона.

7. ИЗМЕНЕНИЕ РЕГИСТРАЦИОННЫХ ДАННЫХ УЧАСТНИКОВ СИСТЕМЫ

7.1. Изменение регистрационных данных Участника Системы, не являющегося Администратором Документооборота или его Представителем, осуществляется на основании заявления об изменении регистрационных данных, подаваемого Участником системы Оператору через Администратора Документооборота или его Представителя в виде документа на бумажном носителе.

7.2. Заявление на изменение регистрационных данных Участника Системы должно содержать сведения в составе, определенном пунктами 6.3 и 6.4 настоящего Регламента, являющиеся актуальными на момент подачи заявления, и информацию о регистрационных данных, утративших свою актуальность.

7.3. В случае изменения регистрационных данных Участника Системы в части их, содержащейся в выданном ему сертификате, осуществляется процедура внеплановой смены ключей усиленной неквалифицированной электронной подписи, определенной Регламентом предоставления Удостоверяющим центром ОАО «ИнфоТеКС Интернет Траст» услуг по созданию и выдаче сертификатов ключей проверки электронных подписей, не являющихся квалифицированными.

7.4. Изменение регистрационных данных Участника Системы, являющегося Администратором Документооборота или его Представителем, осуществляется в порядке, определенном договором об оказании услуг, заключенным между Оператором и Администратором Документооборота.

8. ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

8.1. На основании договора об оказании услуг, заключенного между Оператором и Администратором Документооборота, определяется режим видимости Участников для Администратора Документооборота.

8.2. Если договором об оказании услуг, заключенным между Оператором и Администратором Документооборота, определен открытый режим видимости Участников, то Администратор Документооборота может верифицировать регистрационные данные Участников, зарегистрированных другими Администраторами Документооборота, а регистрационные данные Участников, зарегистрированные Администратором Документооборота, могут быть верифицированы другими Администраторами Документооборота.

8.3. Если договором об оказании услуг, заключенным между Оператором и Администратором Документооборота, определен закрытый режим видимости Участников, то Администратор Документооборота не может верифицировать регистрационные данные Участников, зарегистрированных другими Администраторами Документооборота, а регистрационные данные Участников, зарегистрированные Администратором Документооборота, не могут быть верифицированы другими Администраторами документооборота.

8.4. Система позволяет организовать информационное взаимодействие (Документооборот) между Участниками Системы, выразившими согласие на информационное взаимодействие, в отношении которых Администратором Документооборота или Представителем Администратора Документооборота проведена процедура регистрации в Системе или процедура верификации регистрационных данных Участника в Системе.

8.5. Система позволяет организовать информационное взаимодействие в соответствии параметрами Документооборота, заданными Администратором Документооборота.

8.6. В случае инициирования Администратором Документооборота или Представителем Администратора Документооборота информационного взаимодействия с Участником, регистрация которого в Системе была произведена данным Администратором Документооборота или его Представителем, согласие на информационное взаимодействие с данным Администратором Документооборота или его Представителями подразумевается выраженным Участником в процессе регистрации Участника в Системе, дополнительного подтверждения согласия не требуется.

8.7. В случае инициирования информационного взаимодействия с Участником Системы, регистрация которого в Системе была произведена через иного Администратора Документооборота, Администратор Документооборота или его Представитель должен предварительно произвести верификацию регистрационных данных Участника Системы путем

проверки документов, подтверждающих достоверность регистрационных данных. При выполнении верификации регистрационных данных Участника Системы Администратор Документооборота или его Представитель должен установить личность Участника Системы – физического лица или Уполномоченного сотрудника Участника Системы – юридического лица, а также установить полномочия Уполномоченного сотрудника Участника Системы – юридического лица.

8.8. С момента инициации информационного взаимодействия с Участником Системы, чьи регистрационные данные были верифицированы Администратором Документооборота, Администратор Документооборота принимает на себя все риски в отношениях с данным Участником Системы, и не вправе требовать от Оператора Системы возмещения убытков, причиненных вследствие ненадлежащей регистрации Участника Системы через иного Администратора Документооборота.

8.9. Для получения согласия на информационное взаимодействие от Участника Системы, регистрация которого в Системе была произведена через иного Администратора Документооборота, Участнику Системы направляется код подтверждения согласия на информационное взаимодействие с Администратором Документооборота. Код подтверждения направляется средствами Системы в форме SMS-сообщения на указанный Участником Системы при регистрации номер мобильного телефона, содержащего регистрационные данные Администратора Документооборота, инициирующего информационное взаимодействие. Участник системы выражает согласие на информационное взаимодействие с Администратором Документооборота путем сообщения значения кода подтверждения лицу, проводящему верификацию данных Участника в соответствии с п. 8.4 настоящего Регламента. Информационное взаимодействие с данным Участником Системы возможно только после получения от него кода подтверждения.

9. ЭЛЕКТРОННЫЕ ДОКУМЕНТЫ

9.1. В Системе предусмотрено использование формализованных и неформализованных электронных документов.

9.2. **Формализованные электронные документы.**

9.2.1. Все используемые в Системе формализованные электронные документы предварительно регистрируются в Системе путем включения в реестр формализованных электронных документов с присвоением каждому документу уникального идентификатора.

9.2.2. Для включения документа в реестр формализованных электронных документов Администратор Документооборота должен представить Оператору соответствующую форму электронного документа, подписанную усиленной неквалифицированной подписью Администратора Документооборота.

9.3. **Неформализованные электронные документы.**

9.4. Неформализованные электронные документы не требуют предварительной регистрации в Системе.

9.5. Неформализованные электронные документы формируются Администратором Документооборота в произвольной форме и могут содержать любую информацию, подписать которую предлагается взаимодействующему Участнику Системы.

10. ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА В СИСТЕМЕ

10.1. При необходимости направления взаимодействующему Участнику Системы на подписание электронного документа Администратор Документооборота или его Представитель формирует электронный документ и размещает документ в Системе, определяя конкретные параметры Документооборота. При этом формирование формализованного документа осуществляется непосредственно в Системе путем добавления к зарегистрированной в реестре форме значений переменных параметров документа, имеющих отношение к конкретному взаимодействующему Участнику Системы.

10.2. После размещения электронного документа в Системе Участник Системы, который определен в качестве подписанта документа, оповещается о данном событии следующими способами:

10.2.1. Путем формирования уведомления о поступившем на подписание документе в Личном кабинете Участника Системы.

10.2.2. Путем передачи уведомления о поступившем на подписание документе через информационную систему Администратора Документооборота или его Представителя.

10.2.3. Путем направления на указанный Участником Системы при регистрации номер мобильного телефона SMS-сообщения, которое, в зависимости от параметров Документооборота, может содержать:

- для формализованных документов:
  - наименование Администратора Документооборота или его Представителя;
  - информацию о наименовании, уникальном идентификаторе и значениях переменных параметров формализованного документа;
  - уникальную временную ссылку на поступивший электронный документ для ознакомления;
  - сеансовый ключ доступа к Доверенному сервису электронной подписи;
- для неформализованных документов:
  - наименование Администратора Документооборота или его Представителя;
  - уникальную временную ссылку на поступивший электронный документ для ознакомления;
  - сеансовый ключ доступа к Доверенному сервису электронной подписи.

10.3. Участник Системы может ознакомиться с направленным ему документом одним из следующих способов:

10.3.1. Путем перехода на страницу ознакомления с документом в Системе по уникальной временной ссылке, содержащейся в полученном SMS-сообщении.

10.3.2. Путем перехода на страницу ознакомления с документом в Системе по уникальной временной ссылке, полученной Участником Системы через информационную систему Администратора Документооборота или его Представителя.

10.3.3. Путем авторизации в Личном кабинете Участника Системы с последующим переходом на страницу поступившего документа.

10.3.4. В случае поступления формализованного документа – получив все существенные данные (информацию о наименовании, уникальном идентификаторе и значениях переменных параметров формализованного документа) в составе SMS-сообщения.

10.4. После ознакомления с текстом полученного электронного документа Участник Системы самостоятельно принимает решение о подписании либо отказе от подписания этого документа.

10.5. В случае принятия решения о подписании электронного документа Участник Системы, может произвести его подписание своей неквалифицированной электронной подписью одним из следующих способов (в зависимости от параметров Документооборота):

- путем направления с указанного в регистрационном заявлении Участника Системы номера мобильного телефона SMS-сообщения с сеансовым ключом доступа к Доверенному сервису электронной подписи в ответ на SMS-сообщение, содержащее ключевые параметры подписываемого электронного документа;
- путем ввода в веб-интерфейсе Системы на странице, отображающей содержание подписываемого электронного документа, сеансового ключа доступа к Доверенному сервису электронной подписи, полученного в SMS-сообщении на указанный в регистрационном заявлении Участника номер мобильного телефона. В случае невозможности доставки SMS-сообщения по техническим причинам, сеансовый ключ доступа к Доверенному сервису электронной подписи доставляется в ходе голосового звонка от автоинформатора, заказанного пользователем в веб-интерфейсе Системы на странице, отображающей содержание подписываемого электронного документа.

11. ОБЯЗАННОСТИ СТОРОН

11.1. **Участники Системы обязаны:**

11.1.1. Выполнять требования нормативных правовых документов при осуществлении Документооборота, в отношении которого такие требования установлены.

11.1.2. В случае изменения регистрационных данных, указанных в регистрационных документах, не позднее трех рабочих дней со дня соответствующего изменения, представить Оператору сведения об изменениях в регистрационных данных способом, определенным разделом 7 настоящего Регламента.

11.1.3. Принять все доступные меры для обеспечения конфиденциальности ключевой информации, используемой для доступа к сервисам Системы, включая защиту от несанкционированного доступа к мобильному телефону и SIM-карте с указанным при регистрации абонентским номером.

11.2. **Обязанности Оператора Системы**

11.2.1. Оператор обязан обеспечить функционирование программно-аппаратного комплекса Системы.

11.2.2. Оператор обязан обеспечить конфиденциальность электронных документов, хранящихся в Системе, в том числе обеспечить защиту от несанкционированного доступа.

11.2.3. Оператор обязан осуществлять фиксацию и регистрацию всех событий в Системе и действий, выполняемых Участниками Системы.

11.2.4. В случае получения от Участника Системы сведений об изменении ранее представленных регистрационных данных, Оператор обязан не позднее трех рабочих дней с момента получения такого заявления осуществить внесение изменений в учетную запись Участника.

11.2.5. При проведении регламентных работ по техническому обслуживанию и внесению изменений в Систему Оператор обязан разместить на своем сайте информацию о проведении таких работ с указанием точной даты и времени их начала и окончания не менее чем за три дня до начала проведения работ.

12. ОТВЕТСТВЕННОСТЬ СТОРОН

12.1. За неисполнение или ненадлежащее исполнение обязанностей, определенных настоящим Регламентом Стороны несут ответственность в соответствии с настоящим Регламентом и законодательством РФ.

12.2. Оператор Системы не несет ответственности за содержание и достоверность информации, содержащейся в электронных документах, подписываемых Участниками Системы, а также за какой-либо ущерб, потери и прочие убытки, которые понес Участник Системы по причине несоблюдения им требований настоящего Регламента, а также в следующих случаях:

- нарушения и сбои в работе технических средств Участников Системы, используемых ими для доступа к Системе, в том числе по причине заражения компьютерными вирусами.
- в иных, не зависящих от Оператора Системы, обстоятельствах, в частности, наступивших в результате действий или бездействия Участников Системы.

12.3. Оператор системы несет ответственность за обеспечение безопасности использования электронных подписей Участников в Системе, включая защиту ключей электронной подписи от компрометации, потери, уничтожения, изменения или иного неавторизованного использования, при условии выполнения Участниками Системы обязанностей, предусмотренных п. 11.1.3 Регламента.

12.4. Оператор обязан обеспечить хранение электронных документов, сформированных в результате Документооборота между Участниками в Системе, в течении 10 лет с момента их формирования, а также обеспечить конфиденциальность электронных документов, хранящихся в Системе, в том числе защиту от несанкционированного доступа.

13. КОНФИДЕНЦИАЛЬНОСТЬ

13.1. **Виды конфиденциальной информации**

13.1.1. Ключи электронных подписей Участников Системы.

13.1.2. Ключевая информация, используемая Участниками Системы для доступа к сервисам Системы.

13.1.3. Персональная и корпоративная информация Участников, предоставленная Оператору Системы, не подлежащая распространению в составе сертификата.

13.1.4. Информация, содержащаяся в обращающихся в Системе электронных документах.

13.2. **Виды информации, не относящейся к конфиденциальной**

13.2.1. Информация, не относящаяся к конфиденциальной информации, является открытой информацией.

13.2.2. Информация, включаемая в создаваемые Удостоверяющим центром неквалифицированные сертификаты, не считается конфиденциальной.

13.2.3. Информация, содержащаяся в настоящем Регламенте, не является конфиденциальной.

13.3. **Предоставление конфиденциальной информации**

Оператор Системы не должен раскрывать информацию, относящуюся к конфиденциальной, каким бы то ни было третьим лицам за исключением случаев, требующих раскрытия в соответствии с законодательством РФ.

14. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ

14.1. Возникновение конфликтных ситуаций в связи с осуществлением электронного Документооборота в Системе.

В связи с осуществлением электронного Документооборота возможно возникновение конфликтных ситуаций, связанных с формированием, доставкой, получением, подтверждением получения электронного документа, а также использованием в данных документах электронной подписи. Данные конфликтные ситуации могут возникать, в частности, в следующих случаях:

- оспаривание результатов проверки электронной подписи;

- оспаривание факта создания электронной подписи электронного документа;
- заявление Участника об искажении электронного документа;
- оспаривание факта отправления и/или получения электронного документа;
- иные случаи возникновения конфликтных ситуаций, связанных с использованием Системы.

14.2. Участники принимают все возможные меры для решения возникающих между ними конфликтных ситуаций в рабочем порядке.

14.3. В случае невозможности решения конфликтной ситуации в рабочем порядке Участник, предполагающий возникновение конфликтной ситуации, должен незамедлительно после возникновения конфликтной ситуации направить уведомление о конфликтной ситуации Оператору.

14.4. Уведомление о конфликтной ситуации должно содержать информацию о существе конфликтной ситуации и обстоятельствах, которые, по мнению Участника, свидетельствуют о наличии конфликтной ситуации.

14.5. Уведомление о наличии конфликтной ситуации отправляется в форме электронного документа на адрес электронной почты Оператора, или в форме бумажного документа.

14.6. Оператор обязан не позднее десяти рабочих дней, следующих за днем получением уведомления, проверить наличие обстоятельств, свидетельствующих о возникновении конфликтной ситуации, и направить Участнику информацию о результатах проверки и, в случае необходимости, о мерах, принятых для разрешения возникшей конфликтной ситуации.

15. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ (ДОПОЛНЕНИЙ) В РЕГЛАМЕНТ

15.1. Внесение изменений в Регламент, включая приложения к нему, производится Оператором в одностороннем порядке.

15.2. Регламент с внесенными изменениями публикуется на сайте Оператора https://iitrust.cloud не позднее 3 (трех) рабочих дней с даты утверждения новой редакции Регламента.

15.3. С целью обеспечения гарантированного ознакомления с текстом изменений, внесенных в Регламент, Участник Системы, являющийся юридическим лицом или индивидуальным предпринимателем, обязан не реже 1 (одного) раза в неделю обращаться на сайт Оператора за сведениями о внесенных в Регламент изменениях.

15.4. Все изменения, вносимые в Регламент, вступают в силу и становятся обязательными для Участника Системы, являющегося юридическим лицом или индивидуальным предпринимателем, по истечении 10 (десяти) рабочих дней после утверждения Оператором Системы. В случае несогласия с изменениями Участник Системы, являющийся юридическим лицом или индивидуальным предпринимателем, имеет право расторгнуть договор присоединения к Регламенту в порядке, предусмотренном настоящим Регламентом.

15.5. Уведомление Участника Системы – физического лица об изменениях Регламента осуществляется при входе Участника системы в свой Личный кабинет посредством информационного сообщения в Личном кабинете, либо при направлении Участнику Системы документа на подписание посредством направления Участнику SMS-сообщения. У Участника Системы есть возможность ознакомиться с изменениями в Регламенте путем перехода по ссылке из Личного кабинета или полученного SMS-сообщения. Продолжение работы Участника Системы в Системе после получения уведомления об изменении Регламента означает согласие Участника Системы с изменениями Регламента.

16. ПОРЯДОК РАСТОРЖЕНИЯ ДОГОВОРА ПРИСОЕДИНЕНИЯ

16.1. Участник Системы вправе в одностороннем порядке отказаться от исполнения договора присоединении к Регламенту, уведомив Оператора об этом не позднее, чем за 10 (десять) календарных дней до даты расторжения.

16.2. После расторжения договора присоединения к Регламенту Участник Системы обязан прекратить использование Системы.

16.3. Прекращение действия договора присоединения не освобождает Стороны Регламента от исполнения обязательств, возникших до указанного дня прекращения действия Регламента, и не освобождает от ответственности за его неисполнение либо ненадлежащее исполнение.