

Требования при реализации удаленного доступа работников контрагента к ИТ-инфраструктуре ПАО «Россети Ленэнерго»

1. В настоящем приложении к Договору применяются следующие определения:

1.	Договор	Настоящий договор
2.	Требования	Настоящее приложение к Договору
3.	Общество	Публичное акционерное общество «Россети Ленэнерго» (ПАО «Россети Ленэнерго»), являющееся стороной по Договору
4.	Контрагент	Сторона, с которой ПАО «Россети Ленэнерго» заключило Договор
5.	ИТ-инфраструктура	Совокупность информационных ресурсов, технологий, аппаратного и программного обеспечения, сетевых компонентов, систем хранения и сервисов, обеспечивающих функционирование и управление ИТ-средой ПАО «Россети Ленэнерго»

2. Контрагент обязан.

2.1. В течение 5 (пяти) рабочих дней с даты подписания Договора, предусматривающего удаленный доступ работников Контрагента к ИТ-инфраструктуре, Контрагент представляет план ресурсного обеспечения проекта (далее - План), который становится неотъемлемой частью Договора. План должен содержать: Перечень специалистов (Ф. И. О., должности, квалификация), уровень загрузки каждого специалиста, график вовлечения специалистов.

Обеспечить представление каждым работником, указанным в Плане, согласия на обработку персональных данных по утвержденной форме (форма - приложение к Требованиям), а также предоставить персонализированные телефонные номера этих работников, подтвержденные на портале государственных и муниципальных услуг, для привязки к создаваемым учетным записям в ИТ-инфраструктуре.

Контрагент обязуется выполнять работы силами специалистов, указанных в Плане, с уровнем загрузки не ниже заявленного. Несоответствие фактического объема трудозатрат заявленному в Плане ресурсного обеспечения проекта в течение отчетного периода считается нарушением обязательств по Договору.

2.2. Предоставлять Обществу и актуализировать информацию о персонале, осуществляющим удаленный доступ к ИТ-инфраструктуре.

Не позднее чем за 1 (один) рабочий день до реализации работниками Контрагента удаленного доступа к ИТ-инфраструктуре представить список работников и (или) субподрядчиков, планирующих получать доступ.

В случае любых изменений в составе работников и (или) субподрядчиков

(добавление, замена, исключение) обновленные списки и согласия направляются в Общество в течение 1 (одного) рабочего дня с момента изменений.

Контрагент обязан поддерживать списки в актуальном состоянии на постоянной основе.

2.3. При внесении изменений в ИТ-инфраструктуру Контрагент в течение 7 (семи) рабочих дней с момента их реализации актуализирует техническую документацию по сопровождаемым ИТ-инфраструктурам в полном объеме, включая: обновление архитектурных схем (логической, технической, интеграционной), фиксацию версий и ревизий документации с указанием даты, автора и краткого описания изменений, описание внесенных изменений в функциональность, актуализацию инструкций по эксплуатации, администрированию и аварийному восстановлению, ведение и обновление журнала изменений, передачу Обществу информации о созданных/измененных административных и сервисных учетных записях с указанием их назначения и уровня доступа.

Актуализированная документация передается работникам Общества, ответственным по взаимодействию с Контрагентом по Договору, в течение 1 (одного) рабочего дня с момента исполнения пункта 2.3 Требований в электронном виде с сопроводительным письмом, содержащим перечень внесенных изменений.

Стороны проводят согласование документации в течение 3 (трех) рабочих дней с момента ее передачи. В случае замечаний Общество направляет их Контрагенту в письменной форме.

Контрагент вносит необходимые корректировки и повторно передает документацию на согласование в течение 3 (трех) рабочих дней. Окончательное согласование считается достигнутым после письменного подтверждения со стороны Общества.

До момента согласования документация считается находящейся в статусе «на утверждении» и не подлежит использованию в качестве официальной.

2.4. В случае необходимости осуществления удаленного доступа к ИТ-инфраструктуре Контрагент обязан обеспечить реализацию базовых мер по информационной безопасности в собственной информационной инфраструктуре:

- двухфакторная аутентификация;
- антивирусная защита автоматизированных рабочих мест и серверов;
- защищенное удаленное подключение с использованием средств криптографической защиты информации;
- защита почтовых сервисов от фишинга;
- защищенный обмен файлами и информацией через файловое хранилище;
- обеспечение процесса управления уязвимостями;
- реализация парольной политики (длина пароля должна быть не менее 10 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, А-Z, а-я, а-z), специальные символы (!, », №, %, *, /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов).

2.5. Не допускать (компьютерных атак) воздействия программных и (или) программно-аппаратных средств на ИТ-инфраструктуру, сети электросвязи, используемых Обществом, направленных на нарушение и (или) прекращение функционирования ИТ-инфраструктуры и (или) создания угрозы безопасности ИТ-инфраструктуре.

2.6. Не допускать неправомерный доступ третьим лицам к информации,

полученной от Общества, в том числе ставшей известной в рамках выполнения своих обязательств по Договору, а также не допускать уничтожения такой информации, ее модифицирования, блокирования, копирования, представления и распространения, иных неправомерных действий в отношении такой информации.

2.7. Незамедлительно информировать Общество о (компьютерных инцидентах) фактах возникновения нарушений и (или) прекращения функционирования ИТ-инфраструктуры, сети электросвязи, используемых Контрагентом для исполнения Договора и (или) о нарушениях безопасности обрабатываемой информации Общества, произошедших в результате компьютерного инцидента.

2.8. Незамедлительно информировать Общество о фактах утери информации, полученной от Общества, ставшей известной в рамках выполнения своих обязательств по Договору, в том числе персональных учетных записей, фактах утери средств вычислительной техники, которые использовались для осуществления удаленного доступа к ИТ-инфраструктуре.

2.9. Оказывать содействие Обществу в установлении причин и условий возникновения компьютерных инцидентов, выполнять предписания Общества об устранении нарушений в части соблюдения требований по обеспечению информационной безопасности.

2.10. В течение 5 (пяти) календарных дней с момента возникновения компьютерного инцидента представить отчет с указанием причин и условий возникновения компьютерного инцидента, точного перечня информации, к которой могли получить неправомерный доступ третьи лица в результате компьютерного инцидента.

2.11. В случае нарушения работоспособности ИТ-инфраструктуры (в связи с нарушениями Контрагентом Требований) Контрагент обязан своими силами восстановить ее работоспособность в срок, определенный Обществом.

2.12. Не использовать программное обеспечение для удаленного управления автоматизированным рабочим местом (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop).

2.13. Не использовать средства вычислительной техники, которые используются в личных целях и к которым не применяются корпоративные меры по информационной безопасности.

2.14. Не передавать персональные учетные записи другим работникам Контрагента, не выполняющим соответствующие работы по Договору (не допущенным к ИТ-инфраструктуре), или третьим лицам.

2.15. В случае привлечения субподрядной организации требовать от нее реализации мероприятий, предусмотренных Требованиями.

3. Общество в любое время вправе.

3.1. Запрашивать актуальные списки работников Контрагента и (или) субподрядчиков, планирующих осуществлять удаленный доступ к ИТ-инфраструктуре.

3.2. Проводить проверки соблюдения Контрагентом Требований.

3.3. Запрашивать у Контрагента политики информационной безопасности Контрагента (субподрядчика), результаты внутренних (внешних) аудитов информационной безопасности, результаты тестирования на проникновение

к собственной инфраструктуре, план реагирования на компьютерные инциденты, а также регламент действий работников в случае нештатных ситуаций.

3.4. Ограничить или прекратить доступ работников Контрагента (субподрядчиков) к ИТ-инфраструктуре.

3.5. Требовать от Контрагента возмещения убытков Общества, возникших в результате компьютерного инцидента или в случае получения неправомерного доступа к ИТ-инфраструктуре третьих лиц.

3.6. В случае нарушений Контрагентом Требований ограничить или прекратить ему доступ к ИТ-инфраструктуре.

3.7. Отказаться от исполнения Договора в одностороннем порядке (без обращения в суд) без возмещения Контрагенту убытков в случае нарушения Контрагентом Требований.

При отказе Общества от Договора в соответствии с настоящим пунктом право использования Обществом объектов интеллектуальной собственности, предоставленное Контрагентом Обществу по Договору, не прекращается.

4. Ответственность Контрагента.

4.1. За несоблюдение Требований Контрагент обязан уплатить Обществу штраф в размере 5 (пять) % от общей цены Договора за каждое нарушение.

4.2. За несоблюдение сроков, установленных Требованиями, Контрагент обязан уплатить Обществу штраф в размере 5 (пять) % от общей цены Договора за каждое нарушение и за каждый день просрочки.

4.3. Контрагент обязан возместить Обществу убытки, возникшие в результате компьютерного инцидента или неправомерного доступа третьих лиц к ИТ-инфраструктуре и информации Общества.

4.4. Уплата штрафов и (или) возмещение убытков, предусмотренных настоящим разделом, производится в течение 7 (семи) рабочих дней со дня предъявления требований от Стороны.

4.5. Стороны согласились, что размер оплаты Контрагенту по Договору может быть уменьшен на сумму начисленных штрафов и (или) убытков в соответствии с пунктами 4.1-4.3 Требований.

4.6. Уплата штрафных санкций не освобождает Контрагента от исполнения обязательств по Договору.

ОБЩЕСТВО

КОНТРАГЕНТ

ФОРМА

Согласие на обработку персональных данных для соблюдения требований информационной безопасности

Я, _____ дата рождения _____,
(фамилия, имя, отчество полностью)

документ: _____ серия _____ номер _____ выдан _____
_____ дата _____,

зарегистрированный(-ая) по месту жительства (месту пребывания) по адресу: _____

фактически проживающий(-ая) по адресу: _____

в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» даю Публичному акционерному обществу «Федеральная сетевая компания - Россети» (ПАО «Россети»), зарегистрированному по адресу: г. Москва, ул. Беловежская, д. 4 (далее - Оператор), свое согласие на обработку моих персональных данных: фамилия, имя, отчество; дата рождения; тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство; адрес регистрации (места пребывания, адрес проживания), биометрические персональные данные (фото- и видеоизображение).

Я даю согласие на использование персональных данных в целях исполнения мною требований Оператора по информационной безопасности, а также на хранение персональных данных на электронных носителях.

Настоящее согласие предоставляется мной на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование персональных данных, уничтожение, а также осуществление любых иных действий, предусмотренных законодательством Российской Федерации, в течение 1 (одного) года после истечения допуска к ИТ-инфраструктуре ПАО «Россети».

Настоящее согласие может быть отозвано мной в письменной форме.

Настоящее согласие действует с момента включения меня в список лиц, осуществляющих удаленный доступ к ИТ-инфраструктуре Оператора и в течение 1 (одного) года после прекращения удаленного доступа к ИТ-инфраструктуре Оператора, либо до даты отзыва мною настоящего согласия путем направления Оператору письменного сообщения об указанном отзыве в произвольной форме, если иное не установлено законодательством Российской Федерации.

_____ «__» _____ 20__ г.

Ф. И. О., подпись

дата

Форму согласовали:

ОБЩЕСТВО

КОНТРАГЕНТ

