Приложение 1
к Порядку предоставления удаленного доступа
к информационным ресурсам ПАО «РусГидро»

Требования по обеспечению информационной безопасности при предоставлении контрагентам удаленного доступа к информационным ресурсам ПАО «РусГидро»

РАЗДЕЛ I. ОБЩИЕ ТРЕБОВАНИЯ

1.1. Контрагент должен соблюдать требования по информационной безопасности (кибербезопасности) при осуществлении информационного взаимодействия с ПАО «РусГидро» (далее также Общество) или проведении работ на объектах информатизации Общества в рамках заключенного Договора, применять необходимые и достаточные меры по защите данных, получаемых из / передаваемых в Общество, а также регулярно проводить необходимые мероприятия в течение всего срока действия Договора для обеспечения надлежащего исполнения своих обязательств в области информационной безопасности.

1.2. Контрагент должен обеспечивать конфиденциальность информации ограниченного распространения, в том числе персональных данных, ставшей ему известной в результате осуществления информационного взаимодействия с Обществом при исполнении заключенного Договора, а также информации касающейся информационной инфраструктуры ПАО «РусГидро», средств защиты информации и способов обеспечения информационной безопасности, конфигурацию Континент АП и учетные данные для удаленного доступа. Не раскрывать её третьим лицам, кроме случаев, когда это необходимо для исполнения Договора или требуется в соответствии с законодательством РФ.

Основные требования ПАО «РусГидро» по соблюдению конфиденциальности изложены в Соглашении о конфиденциальности (NDA), которое является неотъемлемой частью заключенного Договора.

1.3. Контрагент обязан подписать Соглашение о конфиденциальности (NDA) до начала работ по Договору с Обществом, приняв обязательства о соблюдения требований информационной безопасности и обязательства о неразглашении сведений конфиденциального характера при осуществлении информационного взаимодействия с ПАО «РусГидро» или проведения работ на объектах информатизации Общества.

РАЗДЕЛ II. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРЕДОСТАВЛЕНИИ УДАЛЕННОГО ДОСТУПА

2.1. Правила и процедуры обеспечения информационной безопасности

2.1.1. Контрагент должен принять и соблюдать требования Политики информационной безопасности ПАО «РусГидро» (в части касающейся) в целях создания контролируемой среды, связанной с защитой конфиденциальности, целостности и доступности информации.

2.1.2. Контрагент должен определить перечень лиц (работников), которым будет предоставлен удаленный доступ к ИР, а также назначить ответственное лицо в качестве своего представителя и контактного лица по всем вопросам, связанным с обеспечением информационной безопасности при осуществлении взаимодействия, а также определить основной и резервный способ связи с таким ответственным лицом. Данную информацию о Контрагенте куратор (менеджер) проекта указывает в форме заявки на удаленный доступ (пункт 3.2.2 Порядка

предоставления удаленного доступа к информационным ресурсам ПАО «РусГидро»).

Перечень лиц (работников) должен быть направлен письмом на бланке организации Контрагента с подписью (рукописной, факсимильной или электронной) назначенного ответственного лица в соответствии с формой из приложения 1 к настоящим Требованиям.

2.1.3 Контрагент должен обеспечить уведомление куратора (менеджера) проекта об изменении в составе работников Контрагента, имеющих учетные записи с предоставленным им удаленным доступом к ИР ПАО «РусГидро», в течение
24 часов с момента наступления такого события.

2.1.4. Контрагент должен обеспечить уведомление КЦИБ Общества (soc@rushydro.ru, гор. тел.: +7 (495) 785-09-65, моб. тел.: +7 (930) 247-24-73) об инцидентах информационной безопасности, зафиксированных в собственной инфраструктуре Контрагента или в инфраструктуре Субподрядчиков, имеющих доступ в инфраструктуру Контрагента, в течение 24 часов.

К инцидентам информационной безопасности относятся события, в том числе, но не ограничиваясь, связанные с:

- несанкционированным доступом к ИР Контрагента и компрометацией информации, в том числе аутентификационной;
- массовым вирусным заражением средств вычислительной техники Контрагента, в том числе вирусами-шифровальщиками;
- несанкционированным или вредоносным сетевым вторжением в инфраструктуру Контрагента;
- распределенными атаками типа «отказ в обслуживании» (DDoS-атаки) на инфраструктуру Контрагента и т.п.

2.1.5. Контрагент несет ответственность за то, чтобы обеспечивать уведомление каждого Субподрядчика о содержании настоящих Требований по обеспечению информационной безопасности и его соблюдение таким Субподрядчиком.

2.1.6. Контрагент должен заключать договоры (соглашения по информационной безопасности) с Субподрядчиками, в которых описаны меры по обеспечению конфиденциальности, доступности и целостности информации, включая меры ответственности и контроля.

2.1.7. При возникновении компьютерных инцидентов, произошедших в ИР Общества с участием Контрагента и/или Субподрядчика, Контрагент должен обеспечить предоставление по запросу ПАО «РусГидро» всей необходимой информации по данному факту и принять участие в проведении расследования.

2.1.8. Контрагент несет ответственность за допущенные его работниками и работниками Субподрядчика нарушения федерального законодательства в области защиты информации, а также за ущерб, причиненный информационной инфраструктуре Общества, при осуществлении удаленного доступа к его ресурсам.

2.1.9. До начала предоставления удаленного доступа Контрагент должен по требованию предоставить в Общество комплект документов, подтверждающих выполнение им требований по информационной безопасности: политику

информационной безопасности, результаты аудитов информационной безопасности, результаты тестирования на проникновение информационной инфраструктуры, план реагирования на компьютерные инциденты, а также регламент действий работников в случае нештатных ситуаций.

2.1.10. Куратор (менеджер) проекта должен проинформировать Контрагента, осуществляющего удаленный доступ к информационной инфраструктуре ПАО «РусГидро», о необходимости реализации следующих базовых мер по информационной безопасности в собственной инфраструктуре:

- двухфакторная аутентификация пользователей;
- 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 12 символов, пароль должен содержать буквы верхнего и нижнего регистра (А-Я, A-Z, а-я, a-z), специальные символы (!, ", N, %, *, /), в пароле не должно быть персонифицированной информации (имен, адресов, даты рождения, телефонов)).

2.2. Требования к информационной инфраструктуре Контрагентов.

2.2.1. Предоставление работнику Контрагента удаленного доступа к ИР производится с использованием АРМ (ПК, ноутбук, планшетный компьютер), принадлежащего Контрагенту.

2.2.2. В обязательном порядке на АРМ должны быть установлены, активированы и настроены следующие СЗИ:

- антивирусное программное обеспечение с действующей лицензией вендора и периодическим автоматическим обновлением антивирусных баз;
- средство защиты сетевого соединения - VPN-клиент СКЗИ «Континент АП» / «Континент ZTN клиент» (предоставляется Обществом).

2.2.3. АРМ, используемые для удаленного доступа к ИР и обработки полученных данных, должны находиться под физическим контролем, для исключения возможности несанкционированного доступа к ним со стороны третьих лиц.

2.2.4. На мобильном устройстве работника Контрагента должно быть установлено и настроено приложение корпоративной системы двухфакторной аутентификации «Multifactor».

2.2.5. Использование Контрагентами программного обеспечения для удаленного управления автоматизированным рабочим местом запрещено (например, TeamViewer, AnyDesk, AmmyAdmin, AeroAdmin, Radmin, LiteManager, Удаленный рабочий стол Chrome, Microsoft Remote Assistance, Microsoft Remote Desktop).

Приложение 1
к Требованиям по обеспечению информационной безопасности
при предоставлении контрагентам удаленного доступа
к информационным ресурсам ПАО «РусГидро»

Форма официального письма Контрагента о направлении сведений
о работниках для предоставления удаленного доступа

(Оформляется на бланке Контрагента)

Директору Департамента
информационных технологий
и цифрового развития
ПАО «РусГидро»

_____
(И.О. Фамилия)

Уважаемый (ая) _____!

На основании

_____

(наименование документа (договор, соглашение), дата документа, номер документа)

прошу создать учетные записи пользователей домена в инфраструктуре ПАО «РусГидро» следующим работникам.

№	Фамилия И.О.	Должность	e-mail	Телефон	Срок действия учетной записи
		...	...	...	...
...	...	...	...	...	...

Указанные в приложении к данному письму работники ознакомлены с Требованиями по обеспечению информационной безопасности при предоставлении контрагентам удаленного доступа к информационным ресурсам ПАО «РусГидро», в том числе с требованиями к составу пароля учетной записи пользователя домена ПАО «РусГидро».

_____	_____	_____
(должность уполномоченного лица Контрагента)	(подпись)	(И.О. Фамилия)