УТВЕРЖДАЮ

Руководитель Органа инспекции
ООО «Консультационно-экспертный центр»

_____С.К. Никулин
«15» марта 2023г.

ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ
Органа инспекции ООО «Консультационно-экспертный центр»

Политика конфиденциальности Органа инспекции Общества с ограниченной ответственностью «Консультационно-экспертный центр» (далее – Орган инспекции, ОИ) является локальным нормативным актом структурного подразделения Общества с ограниченной ответственностью «Консультационно-экспертный центр» (далее - Общество), разработанным в соответствии с требованиями ГОСТ Р ИСО/МЭК 17020-2012. «Национальный стандарт Российской Федерации. Оценка соответствия. Требования к работе различных типов органов инспекции», утвержденного Приказом Росстандарта от 29.11.2012 №1673-ст, и критериями аккредитации, установленными Приказом Минэкономразвития России от 26.10.2020 № 707 «Об утверждении критериев аккредитации и перечня документов, подтверждающих соответствие заявителя, аккредитованного лица критериям аккредитации», на основании норм Гражданского кодекса Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Указа Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», иных нормативны правовых актов Российской Федерации.

1. Общие положения

1.1. Политика конфиденциальности Органа инспекции (далее – Политика конфиденциальности, Политика) регулирует отношения, связанные с обработкой конфиденциальной информации, создаваемой и (или) используемой в деятельности Органа инспекции, в отношении которой Орган инспекции является обладателем информации, в том числе полученной от третьих лиц.

1.2. Настоящая Политика разработана в целях обеспечения сохранения в тайне (неизвестности третьими лицами) информации, отнесенной к конфиденциальной информации Органа инспекции.

1.3. Принцип конфиденциальности обеспечивается тем, что Органа инспекции:

1.3.1. идентифицирует конфиденциальную информацию Органа инспекции;

1.3.2. определяет общие требования по обработке конфиденциальной информации;

1.3.3. определяет порядок доступа к конфиденциальной информации.

1.4. Основными принципами, которыми руководствуется Органа инспекции в вопросах ограничения доступа к конфиденциальной информации, являются:

- законность ограничения доступа;
- обоснованность ограничения доступа;
- своевременность ограничения доступа.

2. Основные понятия

В Политике используются следующие понятия:

2.1. **информация** – сведения (сообщения, данные) независимо от формы

их представления (текстовая, числовая, графическая, аудио, видео, электронная), в том числе:

2.1.1. данные – сведения, зафиксированные в какой-либо форме;

2.1.2. сообщения – сведения в какой-либо форме, передаваемые между участниками информационного взаимодействия;

2.2. **документированная информация** – информация, зафиксированная на материальном носителе (в том числе на бумажной основе) путем документирования с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

2.3. **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;

2.4. **конфиденциальность информации** – требование не разглашать информацию третьим лицам без согласия ее обладателя, обязательное для выполнения лицом, получившим доступ к определенной информации;

2.5. **конфиденциальная информация** – сведения в любой объективной форме, доступ к которым ограничивается в соответствии с Политикой и разглашение которых может нанести материальный, репутационный или иной ущерб интересам Органа инспекции и/или Общества, его работников и контрагентов Общества/заявителей Органа инспекции, и в отношении которой Органом инспекции введен режим конфиденциальности информации.

Возможными формами представления конфиденциальной информации являются:

2.5.1. речевая информация (информация, представленная в виде информативных акустических сигналов, которая озвучивается в том числе устно на встречах или совещаниях) и звуковая информация (информация, представленная в виде информативных акустических сигналов, которая озвучивается посредством звуковоспроизводящих устройств);

2.5.2. информация в электронной форме, размещаемая в информационных системах (обрабатывается на средствах вычислительной техники (ЭВМ) при помощи информационных технологий, представленная в виде информационных массивов, отдельных файлов и баз данных) и (или) передаваемая посредством информационно-телекоммуникационных систем (по каналам связи, локальным или глобальным вычислительным сетям);

2.5.3. недокументированная информация, зафиксированная на различных носителях (на бумажной, магнитной, оптической или другой основе);

2.5.4. документированная информация, зафиксированная на различных носителях (на бумажной, магнитной, оптической или другой основе);

2.5.5. документированная информация, размещаемая в информационных системах, в форме электронного документа.

2.6. **организация работы с документированной конфиденциальной информацией** – организация процессов учета, воспроизведения (копирования), предоставления, исполнения, отправления, классификации, систематизации, подготовки для оперативного и архивного хранения, уничтожения, хранения, проверки наличия и сохранности документированной конфиденциальной информации;

2.7. **персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2.8. **информация, составляющая коммерческую тайну** – техническая, производственная, финансово-экономическая, коммерческая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, и позволяет ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение или получить преимущество на рынке товаров, работ, услуг или получить иную коммерческую выгоду, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим ограничения доступа;

2.9. **иные сведения конфиденциального характера Органа инспекции** – сведения в любой объективной форме, создаваемые и используемые Органом инспекции, а также физическими лицами – исполнителями по гражданско-правовым договорам, работниками при

исполнении трудовых (функциональных) обязанностей, в том числе сведения, составляющие служебную тайну;

2.10. **обладатель информации** – лицо (Общество/Орган инспекции или контрагент/заявитель), самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

2.11. **Заявитель** – контрагент Общества, заказчик, лицо, занимающееся проектированием, изготовлением, поставкой, монтажом, использованием или техническим обслуживанием объектов, инспектируемых Органом инспекции;

2.12. **допуск к конфиденциальной информации** – выполнение обладателем информации (уполномоченными должностными лицами) определенных процедур, связанных с оформлением права на доступ допускаемых лиц к конфиденциальной информации. Получение допуска со стороны допускаемого лица носит добровольный характер и является подтверждением с его стороны выполнения налагаемых обязательств. Наличие допуска предоставляет допускаемому лицу право работать с конфиденциальной информацией в объеме, определяемом обладателем информации;

2.13. **доступ к конфиденциальной информации** – практическая реализация предоставленного допуском права на возможность получения информации и ее использование (получение возможности ознакомления, в том числе с помощью технических средств, обработки, в частности, копирования, модификации или уничтожения);

2.14. **разглашение конфиденциальной информации** – действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя конфиденциальной информации;

2.15. **уничтожение конфиденциальной информации** – действия, направленные на приведение конфиденциальной информации в состояние, исключающее возможность ее использования и восстановления, в том числе посредством физического уничтожения и/ или удаления из памяти электронно-вычислительных машин носителей конфиденциальной информации и их копий;

2.16. **утрата конфиденциальной информации** – наносящее ущерб Органу инспекции и/или Обществу состояние конфиденциальной информации, к которому приводят хищение и/ или потеря носителя конфиденциальной информации, несанкционированное уничтожение носителей конфиденциальной информации или только отображенной в них конфиденциальной информации, искажение или блокирование конфиденциальной информации;

2.17. **утечка конфиденциальной информации** – неправомерный (неразрешенный) выход такой информации за пределы защищаемой зоны ее функционирования в Обществе или установленного круга лиц, имеющих право работать с ней, если этот выход привел к получению информации (ознакомлению с ней) лицами, не имеющими к ней санкционированного доступа. К утечке конфиденциальной информации приводит, в том числе, ее несанкционированное разглашение или распространение;

2.18. **информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

2.19. **информационные ресурсы** – совокупность данных, организованных для получения информации**.** Под информационными ресурсами подразумеваются отдельные документы, массивы документов, базы данных в информационных системах, архивах, хранилищах, в том числе на носителях информации;

2.20. **несанкционированный доступ** – доступ к информации, нарушающий правила разграничения доступа с использованием или без использования штатных средств информационных систем.

3. Порядок отнесения информации к категории конфиденциальной

3.1. Конфиденциальной информацией Органа инспекции признаются следующие сведения:

3.1.1. Персональные данные, обрабатываемые Органом инспекции;

3.1.2. Секреты производства (ноу-хау) и иная информация, составляющая коммерческую и/или служебную тайну Органа инспекции;

3.1.3. Иные сведения конфиденциального характера, признанные Органом инспекции как подлежащие защите, и разглашение которых может нанести материальный, репутационный или иной ущерб Органу инспекции/Обществу, его сотрудникам и контрагентам, в том числе предусмотренные в Приложении №1 к Политике;

3.1.4. Информация о Заявителе (контрагенте, заказчике), полученная не от Заявителя (например, от предъявителя претензии, регулирующих органов), рассматривается как конфиденциальная.

3.2. Ограничение доступа и идентификация в качестве конфиденциальной информации не может быть установлено в отношении следующих сведений:

3.2.1. содержащихся в учредительных документах Общества, документах, подтверждающих факт внесения записей об Обществе в соответствующий государственный реестр, содержащихся в документах, дающих право на осуществление Органом инспекции деятельности в соответствии с областями аккредитации;

3.2.2. о составе имущества Органа инспекции;

3.2.3. о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

3.2.4. о задолженности по выплате заработной платы и социальным выплатам;

3.2.5. о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

3.2.6. о перечне лиц, имеющих право действовать без доверенности от имени Органа инспекции;

3.2.7. о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

3.2.8. общедоступной информации (к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен);

3.2.9. обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена федеральными законами.

3.3. Отношения Органа инспекции и физических лиц, возникающие в связи с обработкой их персональных данных, регулируются Положением об обработке персональных данных Общества с ограниченной ответственностью «Консультационно-экспертный центр».

3.4. Сводный примерный перечень сведений конфиденциального характера Органа инспекции представлен в Приложении №1 к Политике (конфиденциальная информация). Руководители структурных подразделений Общества, работники которых принимают участие в деятельности Органа инспекции и осуществляют процессы обработки конфиденциальной информации, имеют право на подачу заявки на актуализацию указанного перечня.

3.5. Сведения, которые были получены Органом инспекции от третьих лиц и в отношении которых третьими лицами заявлено, что они являются их конфиденциальной информацией, или конфиденциальный характер которых следует из законодательства Российской Федерации, подлежат защите наряду с конфиденциальной информацией Органа инспекции.

3.6. Срок действия режима конфиденциальности в Органе инспекции устанавливается:

3.6.1. для персональных данных, обрабатываемых Органом инспекции, – до прекращения деятельности Общества;

3.6.2. для секретов производства (ноу-хау), иной информации, составляющей коммерческую тайну, служебную тайну, иных сведений конфиденциального характера, – до прекращения деятельности Общества;

3.6.3. для информации, полученной от Заявителей, – в течение срока, определенного соглашением о неразглашении конфиденциальной информации или иным договором, заключенным с Заявителем (контрагентом Общества).

4. Общие требования по обработке конфиденциальной информации

4.1. Обработка конфиденциальной информации включает в себя процессы подготовки и изготовления конфиденциальной информации, организации работы с конфиденциальной информацией и защиты конфиденциальной информации.

4.2. В Органе инспекции в зависимости от форм представления конфиденциальной информации регламентируются следующие направления обработки конфиденциальной информации:

4.2.1. обработка речевой и (или) звуковой конфиденциальной информации;

4.2.2. обработка недокументированной конфиденциальной информации:

– в электронной форме, размещенной в информационных системах или передаваемой посредством информационно-телекоммуникационных систем;

– зафиксированной на различных носителях (на бумажной, магнитной, оптической или другой основе);

4.2.3. обработка документированной конфиденциальной информации:

– размещенной в информационных системах в форме электронного документа;

– зафиксированной на различных носителях (на бумажной, магнитной, оптической или другой основе).

4.3. Требования к обработке конфиденциальной информации зависят от форм представления конфиденциальной информации и в части, не урегулированной Политикой, регламентируются отдельными локальными нормативными актами.

4.4. Деятельность, связанная с обработкой конфиденциальной информации в Органе инспекции, должна включать в себя, в том числе, мероприятия по защите конфиденциальной информации от утраты и утечки, в том числе путем:

4.4.1. разграничения доступа к служебной информации, предоставляемого по конкретной инспекционной работе только определенным сотрудникам, назначаемым для выполнения данной инспекции, или выполняющих иные служебные задания в рамках деятельности Органа инспекции (проведение внутренних аудитов, расследование жалоб и прочее);

4.4.2. установления на компьютерном оборудовании Органа инспекции учетных записей сотрудников с индивидуальными паролями;

4.4.3. электронного хранения информации на сетевых ресурсах Общества с разграничением прав доступа к информации Органа инспекции для учетных записей сотрудников Органа инспекции и иных работников Общества;

4.4.4. оснащения внешних электронных носителей служебной информации Органа инспекции программным обеспечением для защиты информации от несанкционированного доступа;

4.4.5. хранения архивной информации (документов) в служебных помещениях Органа инспекции в металлических шкафах, имеющих замки для ограничения доступа, ключи от которых находятся в сейфе с цифровым кодом доступа. Доступ к цифровому коду от сейфа и ключам от шкафов для хранения архивной информации имеет руководитель Органа инспекции, его заместитель и лицо, назначенное ответственным за ведение архива. Порядок доступа к архивной информации регулируется локальным нормативным актом Органа инспекции;

4.4.6. уничтожения конфиденциальной информации по истечении сроков ее хранения

с составлением соответствующего акта способом в зависимости от формы хранения:

- на электронных носителях - с помощью низкоуровневого форматирования носителей, либо с помощью удаления конфиденциальных данных и перезаписывания на носитель иной информации;

- на бумажных носителях - с помощью уничтожителя бумаг (класса не ниже уровня Р4 согласно DIN 32757-1).

5. Порядок предоставления доступа и работы с конфиденциальной информацией

5.1. Доступ к конфиденциальной информации предусматривает возможность ознакомления с ней и ее обработку, которая заключается в выполнении следующих действий (операций):

5.1.1. чтение (ознакомление);

5.1.2. копирование, хранение, использование, передачу, удаление (уничтожение);

5.2. К лицам, имеющим доступ к конфиденциальной информации без специального допуска в силу должностных обязанностей и ответственным за организацию системы доступа в Органе инспекции относятся:

5.2.1. Руководитель органа инспекции и его заместитель;

5.2.2. Технический директор и его заместитель;

5.2.3. Менеджер по качеству.

5.3. Под допускаемыми к конфиденциальной информации лицами в Органе инспекции понимаются:

5.3.1. работники Органа инспекции и иных структурных подразделений Общества, принимающие участие в работе Органа инспекции;

5.3.2. лица, выполняющие работу или оказывающие услуги Органу инспекции на основании гражданско-правовых договоров;

5.3.3. иные лица (в том числе контрагенты или представители государственных органов).

5.4. Предоставление доступа к конфиденциальной информации возможно в следующих случаях:

5.4.1. конфиденциальная информация необходима для выполнения трудовых обязанностей (в том числе указанных в должностных инструкциях) допускаемых лиц из числа работников Органа инспекции;

5.4.2. конфиденциальная информация необходима для выполнения договорных обязательств допускаемыми лицами из числа указанных в подпунктах 5.4.2- 5.4.3. пункта 5.3 Политики;

5.4.3. конфиденциальная информация Органа инспекции необходима для подготовки ответа уполномоченным лицом структурного подразделения Общества на запросы органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении конфиденциальной информации.

5.5. Работники Органа инспекции, которым для выполнения своих трудовых обязанностей необходимо иметь доступ к конфиденциальной информации, если такая необходимость возникла как при приеме на работу, так и в период работы в Органе инспекции, должны быть ознакомлены с настоящей Политикой, перечнем конфиденциальной информации Органа инспекции, предупреждены об ответственности за разглашение сведений, содержащих конфиденциальную информацию, и должны заключить соглашение или дать письменное обязательство о неразглашении указанных сведений в соответствии с примерной формой, приведенной в Приложении № 2 к Политике.

5.6. Руководители структурных подразделений разъясняют допускаемым лицам из числа работников (в том числе поступающим на работу) особенности порядка обращения с конфиденциальной информацией, том числе с персональными данными. Инструктаж проводится в объеме Политики и других нормативных правовых и локальных нормативных актов, регламентирующих обеспечение сохранности конфиденциальной информации.

5.7. Допускаемые работники получают доступ в объеме, необходимом

для выполнения ими своих трудовых обязанностей, с разрешения руководителя структурного подразделения и на основании прохождения процедуры допуска.

5.8. Лица из числа указанных в подпунктах 5.4.2 – 5.4.3 Политики, допускаемые к конфиденциальной информации, принимают на себя обязательства о неразглашении полученной конфиденциальной информации путем подписания соглашения о неразглашении или по иной предложенной данным лицом форме, согласуемой Органом инспекции.

5.9. Условия доступа представителей органов государственной власти, иных государственных органов, органов местного самоуправления или условия предоставления конфиденциальной информации Органа инспекции по запросам указанных органов определяются в соответствии с законодательством РФ.

5.10. Допуск к обработке конфиденциальной информации имеет право провести должностное лицо Общества, указанное в пунктах 5.2., 5.3. Политики, в пределах своей компетенции.

5.11. Права допускаемых лиц на доступ к конфиденциальной информации регулируются разрешениями указанных должностных лиц, оформленными в документальном (письменном или электронном) виде в отношении непосредственно подчиненных им лиц.

5.12. В Органе инспекции применяются любой из следующих способов документального оформления разрешений на доступ к конфиденциальной информации (формы разрешительных документов):

5.12.1. составление именных (должностных) списков лиц, допускаемых к той или иной конфиденциальной информации Органа инспекции, в том числе содержащейся в ресурсах информационных систем, в обязательном порядке содержащих должности и фамилии лиц и категории сведений (документов), к которым они допускаются, согласно перечню Приложения № 1 к Политике;

5.12.2. оформление разрешения непосредственно на документе (носителе информации) в виде резолюции (поручения), адресованного конкретному лицу;

5.12.3. указание (перечисление) в организационно-распорядительных и иных документах Органа инспекции лиц (их фамилий), которые при решении конкретных производственных и иных задач должны быть допущены к определенной информации, составляющей конфиденциальную информацию Органа инспекции.

5.13. Предоставление конфиденциальной информации третьим лицам, в том числе органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется по распоряжению Руководителя Органа инспекции.

5.14. При передаче конфиденциальной информации контрагенту Общества/заявителю Органа инспекции разрешается использовать только способ, указанный в соглашении о неразглашении конфиденциальной информации, заключенном Обществом с соответствующим контрагентом/заявителем.

6. Обязанности лиц по соблюдению режима конфиденциальности

6.1. Лица, имеющие доступ к конфиденциальной информации, обязаны:

6.1.1. сохранять конфиденциальность информации, к которой они были допущены, обеспечить неразглашение сведений, составляющих конфиденциальную информацию университета, в публикациях, докладах, документации, при экспонировании на выставках, в ходе организационно-технических переговоров, служебных и неслужебных разговоров, а равно любым иным способом;

6.1.2. при работе с конфиденциальной информацией выполнять требования по защите информации, изложенные в локальных нормативных актах Органа инспекции по обеспечению информационной безопасности, в том числе сохранять в тайне свой индивидуальный пароль от компьютерной техники и сервисов личного кабинета (учетной записи), и периодически менять его;

6.1.3. при прекращении или расторжении трудового/гражданско-правового договора передать Руководителю Органа инспекции материальные носители, содержащие конфиденциальную информацию;

6.1.4. сообщать своему непосредственному руководителю или лицу, его замещающему, об утрате или недостаче документов, содержащих конфиденциальную информацию, ключей от сейфов (хранилища), печатей, удостоверений, пропусков, а также о любых иных обстоятельствах, создающих угрозу конфиденциальности информации;

6.1.5. при возникновении необходимости в передаче конфиденциальной информации по электронной почте не осуществлять передачу конфиденциальной информации с использованием иных средств, чем корпоративная электронная почта Органа инспекции (если иное не предусмотрено в отдельном соглашении или обязательстве о неразглашении);

6.1.6. при передаче конфиденциальной информации в электронной форме по корпоративной электронной почте Органа инспекции включить в исходящее письмо и в последующую переписку уведомление о конфиденциальности в следующей форме:

- на русском языке: «*Это электронное сообщение и любые документы, приложенные к нему, содержат конфиденциальную информацию и предназначены исключительно для использования работниками Органа инспекции ООО «Консультационно-экспертный центр», физическим или юридическим лицом, которому они адресованы. Уведомляем Вас о том, что, если это сообщение не предназначено Вам, использование, копирование, распространение информации, содержащейся в настоящем сообщении, а также осуществление любых действий на основе этой информации, не допускается. Если Вы считаете, что Вы получили это электронное сообщение по ошибке, пожалуйста, свяжитесь с отправителем и незамедлительно удалите электронное сообщение и любые вложения с компьютера. Заранее благодарим.*»;

- на английском языке: *«This e-mail and any attachments to it contain confidential information intended only for the use of the Inspection body of LLC «Advisory centre» staff, the individual or entity who they are addressed to. We inform you that if you are not an intended recipient of this e-mail, the use, copying, distribution of the information contained in this message, as well as the conduction of any action based on this information is not allowed. If you believe that you have received this email in error, please contact the sender and immediately delete the email and any attachments from your computer. Thank you in advance.».*

6.2. Лицам, имеющим доступ к конфиденциальной информации, запрещается:

6.2.1. разглашать конфиденциальную информацию (в том числе знакомить с документами и (или) электронными документами, содержащими конфиденциальную информацию) любым лицам, кроме лиц, допущенных к конфиденциальной информации;

6.2.2. размещать конфиденциальную информацию в сети Интернет;

6.2.3. использовать конфиденциальную информацию в передачах по радио и телевидению, в публичных выступлениях;

6.2.4. снимать копии с документов и других носителей информации, содержащих конфиденциальную информацию, производить выписки из них, а равно использовать различные технические средства (фото-, видео- и звукозаписывающую аппаратуру) для регистрации сведений без разрешения руководителя соответствующего структурного подразделения;

6.2.5. осуществлять пересылку конфиденциальной информации, на личные адреса средств коммуникации (электронная почта, мессенджеры, программные средства социальных сетей и т.п.);

6.2.6. использовать без разрешения от непосредственного руководителя и/или руководителя Органа инспекции для хранения и обработки конфиденциальной информации личные ноутбуки, карманные персональные компьютеры, фотоаппараты, видеокамеры, электронные записные книжки, смартфоны, мобильные телефоны и другие цифровые (вычислительные) устройства, имеющие возможность ввода, хранения, накопления, приема, передачи информации;

6.2.7. самовольно подключать периферийные устройства (внешние по отношению к системному блоку компьютера устройства, например: USB-флеш, внешний CD-ROM, внешний жесткий диск, VPN-ключ, e-token) или устанавливать дополнительные любые программные средства, копировать конфиденциальную информацию на личные флеш-карты и иные устройства хранения информации;

6.2.8. использовать для хранения конфиденциальной информации облачные сервисы, за исключением сервисов, контролируемых Органом инспекции.

6.3. Лица, имеющие доступ к конфиденциальной информации, обязаны:

6.3.1. не создавать копии (в том числе электронные) конфиденциальной информации (в том числе на отделяемые (внешние) носители информации) без получения предварительного согласия руководителя Органа инспекции;

6.3.2. определять количество экземпляров документов (в том числе электронных), содержащих конфиденциальную информацию, в строгом соответствии с действительной необходимостью;

6.3.3. использовать при работе с конфиденциальной информацией Органа инспекции, контрагента Общества/заявителя Органа инспекции только средства вычислительной техники (стационарные компьютеры, мобильные устройства), оснащенные средствами защиты, достаточными для обеспечения информационной безопасности в соответствии с требованиями локальных актов;

6.3.4. прекратить обработку конфиденциальной информации на компьютерной технике при обнаружении в последней неисправностей, вирусов, шпионских программ, программ-майнеров, других вредоносных программ и сообщить о выявленных неисправностях своему непосредственному руководителю (или лицу, его замещающему) и руководителю Органа инспекции.

6.4. Ответственными за обеспечение режима конфиденциальности информации является руководитель Органа инспекции.

6.5. При получении Органом инспекции информации, в отношении которой требуется установление режима конфиденциальности, руководитель Органа инспекции обеспечивает принятие всех необходимых мер по установлению и поддержанию режима конфиденциальности информации, указанных в Политике. Если конфиденциальная информация была получена в деятельности нескольких подразделений, меры по установлению и поддержанию режима конфиденциальности информации применяются совместно руководителем Органа инспекции и руководителями указанных подразделений.

6.6. В целях поддержания режима конфиденциальности информации руководитель Органа инспекции в том числе:

6.6.1. обеспечивает учет лиц, получивших доступ к конфиденциальной информации, и (или) лиц, которым такая информация была предоставлена или передана;

6.6.2. уведомляет работника, доступ которого к конфиденциальной информации необходим для выполнения им своих трудовых обязанностей, о конфиденциальном характере раскрываемой работнику информации, обладателями которой являются Органа инспекции или его заявители (контрагенты Общества);

6.6.3. контролирует факт ознакомления под подпись работника с Политикой и иными локальными нормативными актами, направленными на обеспечение конфиденциальности информации в Обществе и с мерами ответственности за их нарушение;

6.6.4. создает работнику необходимые условия для соблюдения им установленного в Органе инспекции режима конфиденциальной информации;

6.6.5. обеспечивает заключение с заявителями Органа инспекции/контрагентами Общества, в том числе с лицами, выполняющими работы (оказывающими услуги) в пользу Органа инспекции на основании гражданско-правовых договоров, содержащих обязательства о неразглашении конфиденциальной информации, или соглашений о неразглашении конфиденциальной информации (Приложение №2);

6.6.6. исполняет иные обязанности, предусмотренные Политикой.

6.7. Если информация, в отношении которой целесообразно установление режима конфиденциальности информации, получена в ходе выполнения работ по договору или реализации соглашения, в целях определения конкретных сведений, подлежащих сохранению в тайне, необходимых мер по защите информации, а также для урегулирования иных вопросов, руководитель подразделения, ответственный за исполнение договора (соглашения) со стороны Общества, по поручению руководителя Органа инспекции обеспечивает

включение в соответствующий договор (соглашение) положений, определяющих взаимные обязательства и ответственность сторон за ее сохранность.

6.8. В договорах с контрагентами Общества (заявителями Органа инспекции) предусматриваются следующие условия:

6.8.1. обязанность Органа инспекции получить предварительное разрешение контрагента о возможности предоставления третьим лицам конфиденциальной информации, обладателем которой является контрагент;

6.8.2. обязанность Органа инспекции уведомить контрагента о случае предоставления по основанному на законе требованию органа государственной власти, иного государственного органа, органа местного самоуправления, конфиденциальной информации, обладателем которой является контрагент, или о случае предоставления такой информации, если это разрешено контрагентом или предусмотрено соглашением (договором) с ним;

6.8.3. право Органа инспекции не получать предварительное разрешение контрагента Общества при предоставлении им конфиденциальной информации, обладателем которой является контрагент, при рассмотрении и подготовке ответов на жалобы, претензии;

6.9. Направление в адрес контрагентов уведомлений, предусмотренных пп. 6.8.1. – 6.8.2. Политики, организуется руководителем Органа инспекции.

6.10. В случае привлечения Органом инспекции в рамках проведения инспекционной деятельности третьих лиц для выполнения части работ (соисполнителей, субподрядчиков) в договоры с такими лицами включаются положения, регламентирующие порядок обеспечения и раскрытия конфиденциальной информации.

6.11. Доступ в служебные (офисные) помещения Органа инспекции имеют только сотрудники Органа инспекции (работники и лица, привлекаемые для выполнения части работ Органа инспекции). Третьи лица могут находиться в помещениях (офисах) Органа инспекции только в сопровождении (присутствии) сотрудника Органа инспекции или только в зоне/ах для посетителей.

6.11.1. Ограничение доступа осуществляется с помощью системы охраны, которая включает: наличие электронных замков на дверях помещений с индивидуальным кодом, выдачу (кодирование) ключей доступа сотрудникам Органа инспекции по распоряжению руководителя Органа инспекции;

6.11.2. При нахождении третьих лиц в служебных (офисных) помещениях Органа инспекции сотрудник Органа инспекции обеспечивает сохранение конфиденциальной информации в тайне, в том числе обеспечивая, чтобы:

- документы, содержащие конфиденциальную информацию, не располагались на рабочих столах /или в местах временного осуществления служебной деятельности в общедоступных местах таким образом, при котором их содержание может стать доступным для третьих лиц;

- мониторы компьютеров (ноутбуков) при выполнении служебной деятельности не должны располагаться таким образом, при котором конфиденциальная информация может стать доступной для третьих лиц.

7. Ответственность за нарушение режима конфиденциальности

7.1. Орган инспекции несет ответственность за нарушение режима конфиденциальности в соответствии с действующим законодательством Российской Федерации, а также условиями заключенных с Заявителями договоров.

7.2. Сотрудники Органа инспекции несет ответственность за нарушение режима конфиденциальности на принципе персональной ответственности, который заключается в том, что каждое лицо, предоставляющее допуск или получившее доступ к конфиденциальной информации должно лично отвечать за свою деятельность, включая любые действия с конфиденциальной информацией и возможные нарушения по обеспечению ее безопасности, т.е. какие-либо случайные или умышленные действия, которые приводят или могут привести к несанкционированной утечке или утрате конфиденциальной информации.

7.3. Лица, разгласившие конфиденциальную информацию, или иным образом нарушившие установленный Политикой порядок доступа, работы, хранения и уничтожения конфиденциальной информации, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

7.4. Нарушением режима конфиденциальности информации признаются, в том числе:

7.4.1. разглашение конфиденциальной информации;

7.4.2. неправомерное использование конфиденциальной информации;

7.4.3. несанкционированный доступ к конфиденциальной информации;

7.4.4. утрата документов и иных материальных носителей, содержащих конфиденциальную информацию;

7.4.5. неправомерное уничтожение документов, содержащих конфиденциальную информацию;

7.4.6. нарушение требований хранения документов, содержащих конфиденциальную информацию;

7.4.7. другие нарушения требований законодательства и настоящей Политики.

8. Заключительные положения

8.1. Контроль за деятельностью Органа инспекции, в том числе на предмет соответствия требованиям законодательства, связанным с режимом конфиденциальности, осуществляют:

- Федеральная служба по аккредитации (Росаккредитация);
- другие уполномоченные органы.

8.2. Выполнение требований настоящей Политики конфиденциальности является обязательным для сотрудников Органа инспекции и работников Общества, принимающих участие в работе Органа инспекции.

Приложение №1
к Политике конфиденциальности
Органа инспекции ООО «Консультационно-экспертный центр»

Перечень конфиденциальной информации
Органа инспекции
Общества с ограниченной ответственностью «Консультационно-экспертный центр»

№	Направления деятельности	Лица, уполномоченные на распоряжение конфиденциальной информацией	Основные категории конфиденциальной информации
1	Орган инспекции	Руководитель органа инспекции и его заместитель; Технический директор и его заместитель; Менеджер по качеству	1. информация о хозяйственно-финансовых отношениях с контрагентами (в том числе условия договорных отношений с ними), о проведении переговоров, переписке с ними; 2. информация, составляющая электронную базу Органа инспекции/Общества, содержащая сведения о структуре баз данных, в том числе, но не исключая: наименование столбцов и строк баз данных, наименование листов; алгоритмы распределения элементов (ячеек) в базах данных; механизмы и алгоритмы работы баз данных; сведения об ошибках и уязвимостях баз данных, а также сведения, полученные в результате работы с базами данных; 3. не являющаяся общедоступной информация о работниках, контрагентах Органа инспекции/Общества (в том числе адреса, телефоны, сведения об имущественных правах, аффилированных лицах, деловых связях, финансовом и экономическом состоянии и т.п.), о деятельности Органа инспекции/Общества; 4. содержание инспекционной деятельности Органа инспекции, работах и их результатах; 5. любые сведения, содержащиеся в документах, электронных сообщениях, электронных документах, за исключением сведений, получаемых из информационных рассылок, направленных на неопределенное или неопределяемое число получателей; 6. сведения о подготовке, принятии и исполнении решений руководства Органа инспекции по вопросам его деятельности; 8. логины (наименования учетных записей) и пароли, используемые сотрудниками Органа инспекции/Общества для доступа в служебные помещения, к информации в электронном виде; 10. содержание заключенных договоров (контрактов), информация, полученная Органом инспекции в рамках исполнения договора (контракта) и определенная по его условиям как конфиденциальная; 11. сведения о совещаниях, проводимых в Органе инспекции, и содержание обсуждаемой на таких совещаниях информации, при условии, что до начала совещания или во время проведения совещания было сделано предупреждение в любой форме о конфиденциальности такого совещания;

			12. информация о личных отношениях работников как между собой, так и с руководством Органа инспекции, сведения о возможных противоречиях, конфликтах внутри коллектива, иная служебная информация, полученные при взаимодействии с работниками Органа инспекции и иными структурными подразделениями Общества, содержание письменных и устных поручениях руководства Органа инспекции; 13. сведения о результатах интеллектуальной деятельности до получения ими правовой охраны / защиты; 15. отчетные документы по результатам внутренних проверок (в т.ч. документы по учету нарушений работников); 16. информация, составляющая коммерческую тайну Общества; 17. оперативные (текущие) документы общего делопроизводства Органа инспекции: внутренние (организационные, распорядительные, информационно-справочные и др.); входящая и исходящая корреспонденция (в том числе в электронном виде); 18. архивные документы Органа инспекции; 19. сведения о порядке и состоянии организации безопасности и системе охраны, пропускном режиме, противопожарной безопасности, систем сигнализации (охранной и АПС) и т.п. в помещениях Органа инспекции; 20. сведения о размере заработной платы работников Органа инспекции; сведения о принятии решений, касающихся материального стимулирования работников, в том числе о процедуре их согласования; 21. положения трудовых договоров (контрактов), заключаемых с работниками Органа инспекции, за исключением сведений, которые не могут относиться к конфиденциальной информации в соответствии с законодательством Российской Федерации; 23. система организации труда в Органе инспекции, за исключением информации, подлежащей обнародованию и предоставлению третьим лицам во исполнение требований действующего законодательства; 24. Финансовая информация, имеющая коммерческую ценность, не содержащаяся в учредительных и иных документах, находящихся в публичном доступе, а также относящаяся к категории ограниченного доступа.

Приложение № 2
к Политике конфиденциальности
Органа инспекции ООО «Консультационно-экспертный центр»

ОБЯЗАТЕЛЬСТВО
о неразглашении конфиденциальной информации
(примерная форма)

Я, _____,
получивший и/или получающий доступ к конфиденциальной информации, именуемый в дальнейшем **«Работник/Сотрудник/Исполнитель»,** принимая во внимание и исходя из того, что:

- между мной и Органом инспекции ООО «Консультационно-экспертный центр» (далее-Орган инспекции) производился, производится и/или будет производиться обмен информацией, в том числе конфиденциальной информацией,
- в период работы/осуществления деятельности в Органе инспекции я получаю, получил и/или будет получать информацию и использовать конфиденциальную информацию, осуществлять доступ к конфиденциальной информации,
- признаю существенной необходимость обеспечения защиты конфиденциальной информации,
- ознакомлен с Политикой конфиденциальности Органа инспекции, с Перечнем конфиденциальной информации Органа инспекции (далее – Конфиденциальная информация) и требованиями законодательства РФ в этой области, в том числе с положениями Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», обязуюсь в течение срока действия трудового договора/гражданско-правового договора с Органом инспекции/Обществом и в течение трех лет с момента его прекращения:

1. не разглашать, не распространять, не передавать и не предоставлять третьим лицам прямо или косвенно любыми возможными способами (в том числе вербально, невербально, письменно; путем предоставления или распространения документированной информации или информации, выраженной на каких-либо материальных носителях, ее демонстрации, путем передачи электронных сообщений и электронных документов) и в любой форме (в том числе в форме текстов, графиков, изображений, рисунков, схем, ссылок, образов, светокопий, фотографий, копий, оригиналов), и объеме Конфиденциальную информацию, а также средства и данные, позволяющие получить доступ к ней, хранить в тайне Конфиденциальную информацию, а также указанные средства и данные, и ограничивать доступ к ним третьих лиц, включая лиц, относящихся к обычному кругу моей семьи;
2. принимать все разумные меры для сохранения Конфиденциальной информации в тайне от любых третьих лиц, воздерживаясь, в частности, от использования технических и технологических средств автоматической авторизации, аутентификации, верификации и/или идентификации в информационных системах, содержащих Конфиденциальную информацию, от использования популярных почтовых сервисов, в том числе в целях пересылки и хранения Конфиденциальной информации, от использования распространенных, скомпрометированных или простых и распространенных ключей доступов (в частности, пары логина и простого и распространенного пароля) и средств однофакторной авторизации, от использования незащищенных или публичных сетей доступа, а также от загрузки Конфиденциальной информации в социальные сети;
3. не использовать Конфиденциальную информацию в целях, не связанных с выполнением должностных обязанностей/договорных обязательств и/или служебных заданий;

не использовать Конфиденциальную информацию, действуя от своего имени или в качестве работника третьего лица, в целях исполнения обязательств перед третьими лицами, а также при реализации любой иной деятельности, напрямую не относящейся к выполнению должностных обязанностей/договорных обязательств и/или служебных заданий;

4. незамедлительно информировать непосредственного руководителя и/или Руководителя Органа инспекции об истребовании у меня Конфиденциальной информации органами государственной власти либо иными лицами.

5. незамедлительно сообщать непосредственному руководителю и/или Руководителю Органа инспекции о возникновении фактов и/или обстоятельств, которые могут привести или привели к разглашению, распространению, предоставлению, передаче третьим лицами Конфиденциальной информации и/или средств и данных, позволяющих получить доступ к ней, в том числе об утрате материальных носителей, содержащих Конфиденциальную информацию, об утрате конфиденциальности средств и данных, позволяющих получить доступ к Конфиденциальной информации, включая ключи доступа (в том числе пары логина и пароля) в информационные системы;.

6. заблаговременно, но не позднее, чем за 2 (два) календарных дня до момента прекращения трудового договора/гражданско-правового договора с Органом инспекции/Обществом:

– возвратить или по указанию непосредственного руководителя и/или Руководителя Органа инспекции уничтожить материальные носители с Конфиденциальной информацией, средствами и данными, позволяющими получить доступ к Конфиденциальной информации;

– удалить с обеспечением недопустимости последующего восстановления информации (в том числе путем устранения теневых отображений данных и многократной перезаписи каждого сектора жесткого диска; без возможности последующего восстановления) со всех используемых мной материальных носителей, облачных хранилищ данных и иных хранилищ информации, не принадлежащих и не контролируемых исключительно Органом инспекции, Конфиденциальную информацию и/или средства и данные, позволяющие получить доступ к Конфиденциальной информации, а при невозможности их удаления, уничтожить такие материальные носители;

– удалить со всех используемых мной ЭВМ, облачных хранилищ данных и иных хранилищ информации, не принадлежащих и не контролируемых исключительно Органом инспекции, электронные файлы с Конфиденциальной информацией, а также средства и данные, позволяющие получить доступ к Конфиденциальной информации, включая различного рода сведения, технические и технологические средства, файлы cookies, ссылки для доступа к Конфиденциальной информации и пр., с обеспечением невозможности их последующего восстановления (в том числе путем устранения теневых отображений данных и многократной перезаписи каждого сектора жесткого диска).

Я предупрежден о том, что в случае нарушения режима конфиденциальности, нарушения требований Политики конфиденциальности Органа инспекции, в том числе за умышленное и/или неосторожное разглашение Конфиденциальной информации, я могу быть привлечен к гражданско-правовой, дисциплинарной, административной и уголовной ответственности в соответствии с законодательством Российской Федерации.

_____	_____	« ___» _____20__ г.
(ФИО)	*(подпись)*	*(дата)*