Утверждено
приказом от 14 мая 2020 № 18/1-ОД

Положение
о защите конфиденциальной информации
ГБУК РО «ИАЦ культуры и туризма»

1. Общие положения

1.1. Положение о защите конфиденциальной информации ГБУК РО «ИАЦ культуры и туризма» (далее соответственно – Положение, Учреждение) регулирует отношения, связанные с обработкой конфиденциальной информации, создаваемой и (или) используемой в деятельности Учреждения в отношении которой Учреждение является обладателем информации.

1.2. Для достижения цели в Положении определяются способы решения следующих задач:

1.2.1. определение конфиденциальной информации Учреждения;

1.2.2. определения общих требований по обработке конфиденциальной информации;

1.2.3. определение разрешительной системы доступа к конфиденциальной информации, как основы ограничения доступа к конфиденциальной информации.

1.3. Основными принципами, которыми руководствуется Учреждение в вопросах ограничения доступа к конфиденциальной информации, являются:

1.3.1. законность ограничения доступа – заключается в выполнении требований законодательства при отнесении информации (сведений, данных) к конфиденциальной информации. При этом учитываются как нормы, предписывающие налагать ограничения на доступ к этим сведениям, так и запрещающие такие ограничения;

1.3.2. своевременность ограничения доступа – заключается в установлении ограничений на разглашение и (или) распространение сведений с момента их получения (разработки) или заблаговременно.

1.4. В соответствии со статьей 6 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» действие Положения направлено на введение в Учреждении разрешительной системы доступа к конфиденциальной информации допускаемых лиц (далее – разрешительная система доступа).

1.5. Положение разработано в соответствии с Гражданским кодексом Российской Федерации, Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», иными нормативными правовыми актами Российской Федерации.

2. Основные понятия, используемые в Положении

В Положении 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 Положением и разглашение которых может нанести материальный, репутационный или иной ущерб интересам Учреждения, его работников.

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 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 Учреждения** – сведения в любой объективной форме, создаваемые и используемые работниками Учреждения, а также физическими лицами – исполнителями по гражданско-правовым договорам, при исполнении трудовых (функциональных) обязанностей;

2.10. **обладатель информации** – юридическое лицо (Учреждение или его контрагент) или физическое лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

2.11. **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;

2.12. **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);

2.13. **разрешительная система доступа** – совокупность правовых норм и требований, устанавливаемых обладателем информации с целью обеспечения правомерного ознакомления допускаемыми лицами с конфиденциальной информацией и ее использования для выполнения функциональных обязанностей. Разрешительная система доступа допускаемых лиц предусматривает установление в Учреждении единого порядка обращения с носителями сведений, составляющих конфиденциальную информацию, определение ограничений на доступ к ним различных категорий работников и иных допускаемых лиц, и степени ответственности за сохранность указанных носителей сведений.

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 Учреждению 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 Учреждении 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;

2.21. **работник Учреждения** – физическое лицо, вступившее в трудовые отношения с Учреждением;

3. Порядок отнесения информации к категории конфиденциальной

3.1. Конфиденциальной информацией Учреждения признаются следующие сведения:

3.1.1. Персональные данные, обрабатываемые Учреждением;

3.1.2. Иные сведения конфиденциального характера, признанные Учреждением как подлежащие защите, и разглашение которых может нанести материальный, репутационный или иной ущерб Учреждению, его работникам.

3.2. Ограничение доступа не может быть установлено в отношении следующих сведений:

3.2.1. содержащихся в учредительных документах Учреждения, документах, подтверждающих факт внесения записей о Учреждении в соответствующий государственный реестр;

3.2.2. о составе имущества Учреждения и об использовании средств соответствующих бюджетов;

3.2.3. о состоянии противопожарной безопасности;

3.2.4. 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;

3.2.5. 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 Учреждения;

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

3.3. Сведения, которые были получены Учреждением 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 Учреждения.

3.4. Режим конфиденциальности информации Учреждения действует:

3.4.1. для персональных данных, обрабатываемых Учреждением, – до прекращения деятельности Учреждения;

3.4.2. для информации, полученной от контрагентов Учреждения, – в течении срока, определенного соглашением о неразглашении конфиденциальной информации или иным договором.

4. Разрешительная система доступа к конфиденциальной информации

4.1. Разрешительная система доступа является частью системы правовых, организационных, технических и иных мер, принимаемых Учреждением к защите конфиденциальной информации.

4.2. Разрешительная система доступа предназначена для решения следующих задач:

4.2.1. определение участников разрешительной системы доступа;

4.2.2. определение условий предоставления доступа и порядка допуска к конфиденциальной информации;

4.2.3. определение порядка работы с конфиденциальной информацией;

4.2.4. определение обязанностей лиц в рамках соблюдения разрешительной системы доступа;

4.2.5. определение степени ответственности лиц.

4.3. Принципы построения разрешительной системы доступа:

4.3.1. надежность, реализуемая принятием мер по исключению возможности несанкционированного доступа посторонних лиц к конфиденциальной информации в обычных и экстремальных условиях;

4.3.2. полнота охвата всех категорий исполнителей и всех категорий конфиденциальной информации;

4.3.3. конкретность, т.е. исключение двоякого толкования, и однозначность решения о допуске к конфиденциальной информации;

4.3.4. производственная необходимость как единственный критерий доступа исполнителя к конфиденциальной информации, а также доступа к конфиденциальной информации представителей органов власти в случаях, определяемых законодательством Российской Федерации;

4.3.5. определенность состава и компетенции должностных лиц, дающих разрешение на доступ исполнителя к конфиденциальной информации, исключение возможности бесконтрольной и несанкционированной выдачи таких разрешений;

4.3.6. строгая регламентация порядка работы с конфиденциальной информацией.

5. Участники разрешительной системы доступа в ГБУК РО «ИАЦ культуры и туризма»

5.1. К лицам, имеющим доступ к конфиденциальной информации без прохождения процедуры допуска в силу должностных обязанностей и ответственным за организацию разрешительной системы доступа в Учреждении относятся:

5.1.1. Директор;

5.1.2. Заместитель директора по связям с общественностью;

5.1.3. Главный бухгалтер;

5.1.4. Ведущий бухгалтер;

5.1.5. Главный юрисконсульт.

5.2. Директор Учреждения вправе делегировать руководителям координируемых структурных подразделений часть своих полномочий в части допуска к конфиденциальной информации в установленном в Учреждении порядке.

5.3. Под допускаемыми к конфиденциальной информации лицами в Учреждении понимаются:

5.3.1. работники Учреждения;

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

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

6. Условия предоставления доступа и порядок допуска к конфиденциальной информации

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

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

6.1.2. конфиденциальная информация необходима для выполнения

договорных обязательств допускаемыми лицами из числа указанных в подпунктах 5.3.1-5.3.3 пункта 5.3 Положения;

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

6.2. Работники Учреждения, 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 Учреждении, должны быть ознакомлены с настоящим Положением, предупреждены об ответственности за разглашение сведений, содержащих конфиденциальную информацию, и должны дать письменное обязательство о неразглашении указанных сведений.

6.3. 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 Положения и других нормативных правовых и локальных нормативных актов, регламентирующих обеспечение сохранности конфиденциальной информации, в том числе персональных данных.

6.4. Допускаемые работники получают доступ в объеме, необходимом для выполнения ими своих трудовых обязанностей, с разрешения руководителя структурного подразделения и на основании прохождения процедуры допуска.

6.5. Лица, допускаемые к конфиденциальной информации, принимают на себя обязательства о неразглашении полученной конфиденциальной информации.

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

6.7. Процесс допуска к конфиденциальной информации направлен на исключение необоснованного расширения круга лиц, допускаемых к конфиденциальной информации, и утечки этой информации, а также доступа к ней лиц, не имеющих на то разрешения полномочных должностных лиц Учреждения.

6.8. Лица, которым необходимо работать с конфиденциальной информацией, могут быть допущены к конфиденциальной информации в случае, если они заявили о необходимости доступа к конфиденциальной информации, относятся к категории допускаемых лиц, прошли процедуру допуска, являющуюся составной частью разрешительной системы доступа к конфиденциальной информации Учреждения.

6.9. Процедуру допуска имеет право провести должностное лицо Учреждения, указанное в пунктах 5.1, 5.2 Положения в пределах своей компетенции.

6.10. Процедура допуска предусматривает в обязательном порядке выполнение следующих мероприятий:

6.10.1. проверка отнесения допускаемого лица к категории допускаемых лиц в соответствии с пунктом 5.3 Положения;

7. Порядок работы с конфиденциальной информацией

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

7.1.1.чтение (ознакомление);

7.1.2.копирование, хранение, использование, передачу, удаление (уничтожение).

7.2.Предоставление конфиденциальной информации третьим лицам, в том числе органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется по распоряжению руководителя структурного подразделения.

7.3.В случае возникновения необходимости передать конфиденциальную информацию третьему лицу, должно быть получено разрешение руководителя структурного подразделения, в деятельности которого получена соответствующая конфиденциальная информация.

7.4.При передаче конфиденциальной информации контрагенту Учреждения разрешается использовать только способ, указанный в соглашении о неразглашении конфиденциальной информации, заключенном Учреждением с соответствующим контрагентом.

8. Обязанности лиц в рамках разрешительной системы доступа

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

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

8.1.2.при прекращении или расторжении трудового договора передать руководителю соответствующего структурного подразделения материальные носители, содержащие конфиденциальную информацию;

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

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

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

8.2.2.размещать конфиденциальную информацию в сети Интернет;

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

8.2.4.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;

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

8.2.6.использовать без разрешения от непосредственного руководителя и согласования представителя Центра информационной безопасности 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;

8.2.7.самовольно подключать периферийные устройства или устанавливать дополнительные любые программные средства, копировать конфиденциальную информацию на личные флеш-карты и иные устройства хранения информации.

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

8.3.1.не создавать копии (в том числе электронные) конфиденциальной информации (в том числе на отделяемые (внешние) носители информации) без получения предварительного согласия руководителя соответствующего структурного подразделения;

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

8.4.В целях поддержания режима конфиденциальности информации руководитель структурного Учреждения подразделения:

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

8.4.2.уведомляет работника, доступ которого к конфиденциальной информации необходим для выполнения им своих трудовых обязанностей, о конфиденциальном характере раскрываемой работнику информации, обладателями которой являются Учреждение или его контрагенты;

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

8.4.4.исполняет иные обязанности, предусмотренные Положением.

8.5.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 охране, необходимых мер по защите информации, а также для урегулирования иных вопросов, руководитель подразделения, ответственный за исполнение договора (соглашения) со стороны Учреждения, обеспечивает включение в соответствующий договор (соглашение) положений, определяющих взаимные обязательства и ответственность сторон за ее сохранность.

9. Ответственность за нарушение режима конфиденциальности информации

9.1. Ответственность за нарушение режима конфиденциальности основывается на принципе персональной ответственности, который заключается в том, что каждое лицо, разрешающее доступ 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.

9.2. Лица, разгласившие конфиденциальную информацию, или иным образом нарушившие установленную Положением разрешительную систему доступа, работы и хранения к конфиденциальной информации, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ.

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

9.3.1. разглашение конфиденциальной информации;

9.3.2. неправомерное использование конфиденциальной информации;

9.3.3. несанкционированный доступ к конфиденциальной информации;

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

9.3.5. неправомерное уничтожение документов, содержащих конфиденциальную информацию;

9.3.6. нарушение требований хранения документов, содержащих конфиденциальную информацию;

9.3.7. другие нарушения требований законодательства и настоящего Положения.