

ПОЛОЖЕНИЕ

об организации работы с персональными данными в муниципальном казенном учреждении «Центр предоставления мер социальной поддержки жителям города Красноярск» (порядок обработки персональных данных работников учреждения и других субъектов персональных данных)

1. Общие положения

1.1. Положение об организации работы с персональными данными в муниципальном казенном учреждении «Центр предоставления мер социальной поддержки жителям города Красноярск» (далее - Положение) определяет цели, содержание и порядок обработки персональных данных работников учреждения и других субъектов персональных данных, меры, направленные на защиту персональных данных, а также процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в области персональных данных в муниципальном казенном учреждении «Центр предоставления мер социальной поддержки жителям города Красноярск» (далее - учреждение).

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, 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», Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, постановлением Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Приказом Федеральной службы по техническому и экспортному контролю России от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», правовыми актами администраций города Красноярск, Уставом учреждения, правилами внутреннего трудового распорядка учреждения.

1.3. Обработка персональных данных в учреждении осуществляется с соблюдением принципов и условий, предусмотренных законодательством Российской Федерации в области персональных данных и настоящего Положения.

1.4. Цель настоящего Положения – осуществление в учреждении обработки:

- персональных данных работников учреждения, в связи с реализацией трудовых отношений, в целях обеспечения кадровой работы, в том числе в целях содействия обучению и должностному росту, учета результатов исполнения должностных обязанностей, обеспечения условий труда, гарантий и компенсаций, а также в целях противодействия коррупции;

- персональных данных граждан в целях реализации в пределах своей компетенции полномочий органов местного самоуправления в области дополнительных мер социальной поддержки населению города Красноярск.

1.5. Для целей настоящего Положения используются следующие основные понятия:

персональные данные (далее - ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

оператор персональных данных (оператор) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись,

систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

автоматизированное рабочее место (АРМ) – комплекс технических и программных средств, предназначенных для решения определённого круга задач;

безопасность персональных данных – состояние защищенности персональных данных, при котором обеспечиваются их конфиденциальность, доступность и целостность при их обработке в информационных системах персональных данных;

вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа или воздействия на информационные ресурсы, заведомо приводящая к уничтожению, блокированию, модификации, копированию информации либо к нарушению работы автоматизированной системы;

защита персональных данных – осуществление комплекса мероприятий по предотвращению несанкционированного распространения (утечки, хищения, копирования), утраты, уничтожения, искажения, подделки, блокирования информации;

информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

информационный ресурс – сведения (сообщения, данные), входящие в состав отдельных документов, массивов документов, баз данных, представленные в электронно-цифровой форме;

конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания;

контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств;

несанкционированный доступ – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

пользователь информационной системы персональных данных (Пользователь ИСПДн) – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования;

средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

2. Классификация персональных данных и субъектов персональных данных

2.1. Учреждение осуществляет обработку персональных данных следующих категорий субъектов персональных данных:

- обработка персональных данных работников учреждения;
- обработка персональных данных граждан в целях исполнения полномочий органов местного самоуправления в области дополнительных мер социальной поддержки населению города Красноярск.

2.2. Обработка персональных данных работников учреждения, осуществляется отделом правовой, кадровой и административной работы учреждения, отделом бухгалтерского учета и отчетности учреждения.

2.3. Обработка персональных данных граждан осуществляется отделом по предоставлению дополнительных мер социальной поддержки учреждения, отделом консультирования и приема документов учреждения.

2.4. Учреждение не осуществляет обработку специальных категорий персональных данных, касающихся расовой и национальной принадлежности, политических взглядов, религиозных и иных убеждений, а также о частной жизни, за исключением случаев, предусмотренных законодательством.

2.5. Лица, уполномоченные на обработку персональных данных в учреждении, обеспечивают обработку персональных данных в соответствии с законодательством Российской Федерации и несут установленную законом ответственность за нарушение режима защиты этих персональных данных.

2.6. Персональные данные в учреждении обрабатываются с использованием информационных систем и без их использования.

2.7. Персональные данные, обрабатываемые в учреждении, подлежат защите от несанкционированного доступа и копирования.

2.8. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации. Реализация требований по обеспечению безопасности персональных данных в информационных системах возлагается на специалистов учреждения, ответственных по своему направлению за выполнение требований по защите информации конфиденциального характера.

3. Порядок обработки персональных данных

3.1. Обработка персональных данных осуществляется после получения согласия субъекта персональных данных, за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

3.2. Обработка персональных данных в учреждении включает в себя: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

3.3. Обработка персональных данных в учреждении осуществляется на основании письменного согласия субъекта персональных данных.

3.4. Обработка персональных данных осуществляется только в пределах контролируемой зоны.

3.5. Информация, содержащая персональные данные, при передаче по внешним каналам связи должна быть зашифрована или упакована в файлы, защищенные паролем. Передача данной информации внутри локальной сети должна быть защищена групповыми политиками и разграничением доступа.

3.6. Электронные носители информации, содержащие персональные данные, регистрируются в журнале учета электронных носителей персональных данных.

3.7. Приказом руководителя учреждения назначаются сотрудники, ответственные за защиту персональных данных, администратор информационной безопасности и

утверждается перечень лиц, допущенных к обработке персональных данных, с указанием полномочий доступа к ресурсам учреждения.

3.8. Сотрудники учреждения перед допуском к обработке персональных данных в обязательном порядке подписывают обязательство о неразглашении информации, содержащей персональные данные.

3.9. Обработка персональных данных в ИСПДн осуществляется специалистами учреждения в соответствии с инструкциями по работе в ИСПДн.

3.10. Комиссия по защите персональных данных и конфиденциальной информации в соответствии с утверждаемым ежегодно планом внутренних проверок режима защиты персональных данных проводит мероприятия по проверкам соблюдения режима защиты персональных данных, результат проверки фиксируется в журнале внутренних проверок.

3.11. Сотрудники учреждения, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с Положением.

4. Порядок обработки, хранения и использования персональных данных работников учреждения

4.1. Персональные данные работников учреждения обрабатываются в связи с реализацией трудовых отношений, в целях обеспечения кадровой работы, в том числе в целях содействия обучению и должностному росту, учета результатов исполнения должностных обязанностей, обеспечения условий труда, гарантий и компенсаций, а также в целях противодействия коррупции.

4.2. В целях, указанных в пункте 4.1 настоящего Положения, обрабатываются персональные данные работников учреждения следующего содержания:

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- сведения о трудовой деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- сведения об ученой степени;
- информация о владении иностранными языками, степень владения;
- фотография;
- информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- информация об ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения заработной платы;
- номер расчетного счета;
- номер банковской карты;

- иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 4.1 настоящего Положения.

4.3. Положения настоящего раздела распространяются на лиц, претендующих на трудоустройство в учреждение.

4.4. Персональные данные работников учреждения хранятся в отделе правовой, кадровой и административной работы учреждения, отделе бухгалтерского учета и отчетности учреждения на бумажных носителях с ограниченным доступом.

Исключение возможности несанкционированного доступа к персональным данным при их хранении обеспечивается:

- запретом доступа к персональным данным всем, кроме лиц, определенных в соответствии с пунктом 2.5. настоящего Положения;
- хранением информации на материальных носителях в специальных шкафах, сейфах;
- запретом нахождения посторонних лиц в служебных помещениях учреждения, в которых располагаются соответствующие шкафы, сейфы, персональные компьютеры, в отсутствие лиц, определенных в соответствии с пунктом 2.5. настоящего Положения.

На личных делах работников гриф ограничения доступа не ставится.

Уполномоченным лицам не разрешается, покидая помещение, оставлять какие-либо документы, содержащие персональные данные, на столе, оставлять шкафы, сейфы, в которых находятся материальные носители с персональными данными, незапертыми.

4.5. В отделах учреждения может быть список работников с указанием биографических данных каждого из них (год рождения, место жительства, домашний, сотовый телефоны и другое).

4.6. Работник имеет право знакомиться только со своими персональными данными.

4.7. Начальник отдела правовой, кадровой и административной работы учреждения, начальник отдела бухгалтерского учета и отчетности учреждения или заместитель начальника отдела бухгалтерского учета и отчетности учреждения и исполняющий обязанности начальника отдела правовой, кадровой и административной работы учреждения вправе передавать персональные сведения работников в другие отделы учреждения в случаях, установленных законодательством.

4.8. Личные дела работников могут выдаваться на рабочие места руководителю учреждения, заместителю руководителя учреждения. Передача осуществляется уполномоченным лицом. Передача личных дел руководителю учреждения через третьих лиц не допускается.

Ознакомление лиц, включенных в перечень, определенный в соответствии с пунктом 3.7. настоящего Положения, с личными делами работников, а также работника с его личным делом осуществляется в помещении отдела правовой, кадровой и административной работы учреждения в присутствии сотрудника, ответственного за сохранность и ведение личных дел (далее - исполнитель).

4.9. На рабочем столе исполнителя всегда должен находиться только тот объем документов, с которым он в настоящий момент работает. Документы, с которыми закончена работа, немедленно подшиваются в соответствующее личное дело.

4.10. Работник обязан сообщать об уточнении (изменении и дополнении) своих персональных данных.

Уточнение персональных данных (изменение и дополнение) осуществляется на основании приказов по личному составу и документов, представляемых работниками.

По устному заявлению работника могут быть уточнены (изменены и дополнены) следующие персональные данные: номер телефона (домашний, сотовый).

4.11. При выдаче справки с места работы необходимо удостовериться в личности работника, которому эта справка выдается. Не допускается выдавать ее родственникам или сослуживцам лица, которому требуется справка. Справка подписывается руководителем учреждения (лицом, его замещающим, либо лицом им уполномоченным) и заверяется печатью. Справку на подписание представляют уполномоченные лица.

4.12. Во время приема работника учреждения уполномоченные лица не должны выполнять функции, не связанные с приемом, вести служебные и личные переговоры, в том числе по телефону, о персональных данных других работников. На столе у работника, ведущего прием, не должно быть никаких документов, содержащих персональные данные, за

исключением документов, содержащих персональные данные работника учреждения, находящегося на приеме.

4.13. Руководитель учреждения и начальник отдела правовой, кадровой и административной работы учреждения в целях обеспечения защиты и надлежащего хранения и использования персональных данных работника обязаны:

- обеспечить защиту персональных данных от неправомерного их использования или утраты в порядке, установленном законодательством и настоящим Положением;
- ознакомить работника с его правами в области защиты персональных данных;
- обеспечить работнику доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством;
- осуществлять иные действия, предусмотренные законодательством.

4.14. В целях обеспечения защиты персональных данных, отраженных в личном деле, карточке Т-2 работника учреждения, работник имеет право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);
- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных законодательством;
- требовать исключения или исправления неверных или неполных персональных данных. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требовать уведомления всех лиц, которым были ранее сообщены неверные или неполные персональные данные, обо всех произведенных в них изменениях или исключениях из них;
- обжаловать в установленном порядке действия уполномоченных лиц;
- осуществлять иные права, предусмотренные действующим законодательством.

5. Порядок обработки персональных данных граждан в целях исполнения полномочий органов местного самоуправления в области дополнительных мер социальной поддержки населению города Красноярск

5.1. В учреждении обработка персональных данных осуществляется в целях исполнения полномочий органов местного самоуправления в области дополнительных мер социальной поддержки населению города Красноярск.

5.2. Персональные данные граждан, обратившихся в учреждение лично, а также направивших индивидуальные или коллективные письменные обращения или обращения в форме электронного документа, обрабатываются в целях рассмотрения указанных обращений.

В соответствии с законодательством Российской Федерации в учреждении подлежат рассмотрению обращения граждан Российской Федерации, иностранных граждан и лиц без гражданства.

5.3. В целях, указанных в пункте 5.1 настоящего Положения, обрабатываются персональные данные следующего содержания:

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- сведения о состоянии здоровья;

- сведения о трудовой деятельности;
- реквизиты расчетного счета;
- номер банковской карты;
- иные персональные данные, необходимые для достижения целей, предусмотренных пунктом 4.1 настоящего Положения.

5.4. Во время приема посетителей уполномоченные лица не должны выполнять функции, не связанные с приемом, вести служебные и личные переговоры, в том числе по телефону, о персональных данных иных посетителей. На столе у работника, ведущего прием, не должно быть никаких документов, содержащих персональные данные, за исключением документов, содержащих персональные данные посетителя.

6. Объекты защиты ИСПДн

6.1. Объектами защиты являются – информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты, безопасность которых должна обеспечиваться системой защиты персональных данных в ИСПДн учреждения. Объекты защиты каждой ИСПДн включают:

- персональные данные субъектов ПДн;
- технологическая информация;
- программно-технические средства обработки;
- средства защиты ПДн;
- каналы информационного обмена и телекоммуникации;
- объекты и помещения, в которых размещены компоненты ИСПДн.

6.2. Перечень персональных данных субъектов ПДн :

6.2.1. Перечень персональных данных, обрабатываемых в учреждении в связи с реализацией служебных или трудовых отношений, в целях обеспечения кадровой работы, в том числе в целях содействия обучению и должностному росту, учета результатов исполнения должностных обязанностей, обеспечения условий труда, гарантий и компенсаций, а также в целях противодействия коррупции:

- фамилия, имя, отчество (в том числе предыдущие фамилии, имена и (или) отчества, в случае их изменения);
- число, месяц, год рождения;
- место рождения;
- информация о гражданстве (в том числе предыдущие гражданства);
- вид, серия, номер документа, удостоверяющего личность, наименование органа, выдавшего его, дата выдачи;
- адрес места жительства (адрес регистрации, фактического проживания);
- номер контактного телефона или сведения о других способах связи;
- реквизиты страхового свидетельства государственного пенсионного страхования;
- идентификационный номер налогоплательщика;
- реквизиты страхового медицинского полиса обязательного медицинского страхования;
- реквизиты свидетельства государственной регистрации актов гражданского состояния;
- семейное положение, состав семьи и сведения о близких родственниках (в том числе бывших);
- сведения о трудовой деятельности;
- сведения о воинском учете и реквизиты документов воинского учета;
- сведения об образовании, в том числе о послевузовском профессиональном образовании (наименование и год окончания образовательного учреждения, наименование и реквизиты документа об образовании, квалификация, специальность по документу об образовании);
- сведения об ученой степени;
- информация о владении иностранными языками, степень владения;
- медицинское заключение по установленной форме об отсутствии у гражданина заболевания, препятствующего поступлению на муниципальную службу или ее прохождению;

- фотография;
- информация, содержащаяся в трудовом договоре, дополнительных соглашениях к трудовому договору;
- информация о классном чине муниципальной службы, государственной гражданской службы, дипломатическом ранге, воинском или специальном звании, классном чине правоохранительной службы, классном чине гражданской службы субъекта Российской Федерации и т.д.;
- государственные награды, иные награды и знаки отличия;
- сведения о профессиональной переподготовке и (или) повышении квалификации;
- информация о ежегодных оплачиваемых отпусках, учебных отпусках и отпусках без сохранения денежного содержания;
- номер расчетного счета;
- номер банковской карты;
- иные персональные данные.

6.2.2. ИСПДн «Адресная социальная помощь».

Перечень персональных данных субъектов ПДн:

- фамилия, имя, отчество;
- дата рождения;
- место рождения;
- гражданство;
- контактный телефон;
- адрес регистрации места жительства и фактического проживания;
- паспортные данные;
- идентификационный номер плательщика;
- страховое свидетельство обязательного пенсионного страхования;
- полис обязательного медицинского страхования;
- свидетельство о рождении;
- справка об инвалидности;
- доходы;
- информация о видах деятельности (вид и срок деятельности);
- семейное положение и состав семьи (муж/жена, дети);
- сведения об образовании;
- данные об удостоверениях, наградах, медалях, поощрениях, почетных званиях;
- сведения об опекунах;
- дата и место участия в боевых действиях;
- данные о банковских лицевых счетах;
- данные о жилье (характеристики жилья, квартплата);
- номер финансово-лицевого счета

6.2.3. ИСПДн «1С: Зарплата и Кадры».

Перечень персональных данных субъектов ПДн:

- фамилия, имя, отчество;
- дата рождения;
- место рождения;
- гражданство;
- адрес регистрации места жительства и фактического проживания;
- паспортные данные;
- контактный телефон;
- идентификационный номер плательщика;
- страховое свидетельство обязательного пенсионного страхования;
- информация о видах деятельности (вид и срок деятельности);
- семейное положение и состав семьи (муж/жена, дети);
- сведения об образовании;
- данные об удостоверениях, наградах, медалях, поощрениях, почетных званиях;
- стаж;
- оклад;
- зарплатный счет;
- данные о банковских лицевых счетах;

6.2.4. ИСПДн «1С: Бухгалтерия».

Перечень персональных данных субъектов ПДн:

- фамилия, имя, отчество;
- счет карты;
- расчетный счет;
- паспортные данные.

6.2.5. ИСПДн ««CompanyMedia».

Перечень персональных данных субъектов ПДн:

- фамилия, имя, отчество;
- контактный телефон;
- адрес проживания (регистрации);
- электронная почта.

6.3. Технологическая информация, подлежащая защите, включает:

- управляющую информацию (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- технологическую информацию средств доступа к системам управления (аутентификационная информация, ключи и атрибуты доступа и др.);
- информацию на съемных носителях информации (бумажные, магнитные, оптические и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами или средств доступа к этим системам управления;
- информацию о средствах защиты ПДн, их составе и структуре, принципах и технических решениях защиты;
- информационные ресурсы (базы данных, файлы и другие), содержащие информацию о информационно-телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах;
- служебные данные (метаданные), появляющиеся при работе программного обеспечения, сообщения и протоколы межсетевого взаимодействия, в результате обработки информации.

6.4. Программно-технические средства включают в себя:

- общесистемное и специальное программное обеспечение (операционные системы, СУБД, клиент-серверные приложения и другие);
- резервные копии общесистемного программного обеспечения;
- инструментальные средства и утилиты систем управления ресурсами ИСПДн;
- аппаратные средства обработки ПДн (рабочие станции и сервера);
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.).

6.5. Средства защиты ПДн состоят из аппаратно-программных средств включают в себя:

- средства управления и разграничения доступа пользователей;
- средства обеспечения регистрации и учета действий с информацией;
- средства, обеспечивающие целостность данных;
- средства антивирусной защиты;
- средства межсетевого экранирования;
- средства анализа защищенности;
- средства обнаружения вторжений;
- средства криптографической защиты ПДн, при их передачи по каналам связи сетей общего и (или) международного обмена.

6.6. Каналы информационного обмена и телекоммуникации являются объектами защиты, если по ним передаются обрабатываемая и технологическая информация.

6.7. Объекты и помещения являются объектами защиты, если в них происходит обработка обрабатываемой и технологической информации, установлены технические средства обработки и защиты.

7. Порядок доступа работников учреждения к информационным системам, содержащим персональные данные, используемым в учреждении

7.1. Разграничение прав пользователей, а так же их уровень прав доступа к обрабатываемым персональным данным, осуществляется исходя из характера и режима обработки персональных данных в ИСПДн. Руководители и специалисты учреждения должны иметь доступ только к той ИСПДн («Адресная социальная помощь» (ИС «АСП») учреждения; «1С зарплата»; «1С бухгалтерия»), которая необходима им для выполнения служебных обязанностей.

7.2. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику учреждения, допущенному к работе с конкретным информационным ресурсом или ИСПДн учреждения, должна быть сопоставлена учетная запись пользователя, под которым он будет регистрироваться и работать в системе. Использование несколькими сотрудниками одного и того же имени пользователя («группового имени») запрещено.

7.3. Процедура регистрации (создания учетной записи) пользователя для сотрудника учреждения и предоставления ему (или изменения его) прав доступа к информационным ресурсам и ИСПДн инициируется заявкой заместителя руководителя учреждения согласно приложению 1 к Положению.

7.3.1. В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач и полномочий в конкретных ИСПДн).

7.3.2. Заявку визирует руководитель учреждения, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач.

7.3.3. Затем начальник отдела по предоставлению дополнительных мер социальной поддержки учреждения и начальник отдела правовой, кадровой и административной работы учреждения рассматривает представленную заявку и подписывает задание администратору информационной безопасности, администратору ИСПДн на внесение необходимых изменений в списки пользователей.

7.3.4. На основании заявки администратор информационной безопасности сети в соответствии с формулярами указанных задач, и документацией на средства защиты сетевых операционных систем производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля и заявленных прав доступа к сетевым ресурсам, включению его в соответствующие задачи группы пользователей и другие необходимые действия. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в три месяца.

7.3.5. Администратор ИСПДн производит необходимые операции по созданию (удалению) учетной записи пользователя в ИСПДн, присвоению ему начального значения пароля и заявленных прав в соответствии с заявкой. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в три месяца.

7.3.6. После внесения изменений в списки пользователей администратор информационной безопасности должен обеспечить соответствующие категориям защиты указанных рабочих станций настройки средств защиты. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписями исполнителей – администратора информационной безопасности и администратора ИСПДн.

7.3.7. Сотруднику, зарегистрированному в качестве нового пользователя системы, под роспись сообщается имя пользователя и пароль, который он обязан сменить при первом же входе в систему (при первом подключении к ИСПДн).

7.3.8. Работнику учреждения запрещается разглашать, передавать кому-либо свой персональный пароль.

7.3.9. Исполненная заявка хранится в отделе правовой, кадровой и административной работы учреждения.

8. Порядок резервирования и восстановления работоспособности средств вычислительной техники и средств защиты информации, баз данных ИСПДн

8.1. Порядок резервирования и восстановления работоспособности СВТ и средств защиты информации (далее – Порядок) определяет действия, связанные с функционированием ИСПДн учреждения, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

8.2. Действие настоящего Порядка распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.

8.3. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается администратор безопасности учреждения.

8.4. Ответственным за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается ответственный за обеспечение защиты персональных данных.

8.5. Под Инцидентом понимается происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

8.6. В сроки, не превышающие одного рабочего дня, ответственный за реагирование сотрудник учреждения, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры согласуются с вышестоящим руководством.

8.7. Все критичные помещения учреждения (помещения, в которых размещаются элементы ИСПДн и средства защиты) должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

8.8. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

8.9. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания.

8.10. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID (резервированный массив независимых жестких дисков).

8.11. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (жесткий диск, и т.п.).

8.12. Процедуры резервного копирования должны производиться в соответствии с режимом резервного копирования.

8.13. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования; процедура резервного копирования должна быть зафиксирована в журнале электронных носителей персональных данных.

8.14. Носители должны храниться в негорючем шкафу или помещении, оборудованном системой пожаротушения.

9. Сроки обработки и хранения персональных данных

9.1. Сроки обработки персональных данных в учреждении определяются в соответствии с законодательством Российской Федерации.

9.2. Сроки хранения персональных данных в учреждении определяются в соответствии со сроками, установленными приказом Минкультуры РФ от 25 августа 2010 г. № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и

организаций, с указанием сроков хранения», и утверждаются руководителем учреждения в номенклатуре дел, или договором, стороной которого является субъект персональных данных.

9.3. Порядок организации хранения персональных данных определяется в соответствии с правилами организации хранения, комплектования, учета и использования документов Архивного фонда Российской Федерации и других архивных документов в органах государственной власти, органах местного самоуправления и организациях, утвержденных приказом Министерства культуры Российской Федерации от 31.03.2015 № 526.

9.4. Обрабатываемые персональные данные подлежат уничтожению, блокированию, обезличиванию, изменению в порядке и сроки, указанные законодательством Российской Федерации.

9.5. При необходимости уничтожения части персональных данных, содержащихся на бумажном носителе, с указанного носителя предварительно копируются сведения, не подлежащие уничтожению, затем уничтожается сам носитель.

9.6. Факт уничтожения персональных данных оформляется в форме акта.

10. Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований

10.1. Уничтожение персональных данных - это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) на материальных носителях.

10.2. При достижении целей обработки или наступлении иных законных оснований персональные данные, содержащиеся на материальных носителях и в информационных системах, подлежат уничтожению.

10.3. Отбор документов, содержащих персональные данные и подлежащих уничтожению, осуществляется, а уничтожение организуется экспертной комиссией учреждения по подготовке документов к архивному хранению.

10.4. Уничтожение персональных данных может осуществляться путем:

- обезличивания персональных данных;
- уничтожения материального носителя, содержащего персональные данные (для бумажных носителей) методом измельчения на мелкие части, путем сжигания или же другим способом, исключающим возможность дальнейшего восстановления информации.
- физического уничтожения частей носителей информации, разрушение или сильная деформация (для CD/DVD-дисков, USB-накопителей, Flash-носителей и т.д.);
- стирания с помощью сертифицированных средств уничтожения информации (для электронных документов).

11. Рассмотрение запросов субъектов персональных данных или их представителей

11.1. Субъект персональных данных имеет право на получение в учреждении информации, касающейся обработки его персональных данных в соответствии с частью 7 статьи 14 Федерального закона от 27.07.2006 152-ФЗ «О персональных данных» (далее – Закон), в том числе содержащей:

- подтверждение обработки персональных данных учреждением;
- правовые основания и цели обработки;
- цели и способы обработки персональных данных;
- наименование и место нахождения учреждения, сведения о лицах (кроме работников учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с учреждением или на основании федерального закона «О персональных данных»;
- обрабатываемые персональные данные, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки персональных данных, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных федеральным законом;

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению учреждения, если обработка поручена или будет поручена такому лицу (на основании законодательства о персональных данных);

- иные сведения, предусмотренные федеральным законом «О персональных данных».

11.2. Информация, указанная в пункте 11.1 настоящего Положения, должна быть предоставлена субъекту персональных данных или его представителю в доступной форме, в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

11.3. Сведения, указанные в пункте 11.1 настоящего Положения, предоставляются субъекту персональных данных или его представителю при обращении либо при получении от него запроса. Запрос на предоставление информации должен содержать:

- сведения о документе (серия, номер, дата выдачи, выдавший орган), удостоверяющем личность субъекта персональных данных или его представителя;

- сведения, подтверждающие участие субъекта персональных данных в отношениях с учреждением (номер и дата договора и др.), либо сведения, иным образом подтверждающие факт обработки персональных данных в учреждении;

- подпись субъекта персональных данных или его представителя.

11.4. Ведение делопроизводства, регистрация запросов субъектов персональных данных и их представителей осуществляется в соответствии с правовыми актами администрации города.

11.5. После получения запрос проверяется на повторность. Повторный запрос возможен в сроки и в порядке, предусмотренные частями 4, 5 статьи 14 Федерального закона «О персональных данных».

11.6. Учреждение назначает должностных лиц, ответственных за обработку запросов субъектов персональных данных и их представителей.

11.7. Ответственные за обработку запросов обязаны:

- внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы или организовать проверку фактов, изложенных Заявителем, принять другие меры для объективного разрешения поставленных субъектом персональных данных и их представителей вопросов, выявления и устранения причин и условий, порождающих факты нарушения законодательства о персональных данных;

- принимать законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;

- сообщать в письменной форме субъектам персональных данных и их представителям о принятых решениях со ссылками на законодательство Российской Федерации, а в случае отклонения разъяснять также порядок обжалования принятого решения.

11.8. Учреждение предоставляет безвозмездную возможность ознакомления с персональными данными, вносит в них необходимые изменения, уничтожает их, уведомляет о внесенных изменениях и принятых мерах в соответствии с частью 3 статьи 20 Федерального закона «О персональных данных».

11.9. В случае отказа в предоставлении информации должное лицо, ответственное за обработку готовит мотивированный ответ учреждения в письменной форме в соответствии с частью 2 статьи 20 Федерального закона «О персональных данных».

11.10. В случае выявления неправомерной обработки персональных данных должностные лица учреждения обязаны осуществить блокирование этих данных на период проверки в соответствии с частью 1 статьи 21 Федерального закона «О персональных данных».

11.11. Уточнение персональных данных осуществляется в соответствии с частью 2 статьи 21 Федерального закона «О персональных данных».

11.12. При необходимости для проверки изложенных в запросах фактов проводится внутренний контроль соответствия обработки персональных данных требованиям к их защите.

11.13. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы субъектам персональных данных и их представителей.

12. Порядок доступа в помещения учреждения, в которых ведется обработка персональных данных

12.1. Для помещений учреждения, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

12.2. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только работники учреждения, уполномоченные на обработку персональных данных.

12.3. Нахождение лиц, не являющихся уполномоченными лицами на обработку персональных данных, в помещениях, в которых обрабатываются персональные данные, возможно только в сопровождении уполномоченного на обработку персональных данных работника учреждения.

12.4. Доступ в помещения, в которых осуществляется обработка персональных данных, разрешается только в рабочее время. Доступ в указанные помещения в нерабочее время возможен только по письменной заявке работника, согласованной с его непосредственным руководителем и имеющей разрешающую резолюцию руководителя учреждения.

12.5. Последний работник, покидающий помещение, в котором осуществляется обработка персональных данных, обязан закрыть его на ключ, при этом запрещается оставлять ключ в замке помещения.

12.6. Работники учреждения, имеющие право доступа в помещение, в котором осуществляется обработка персональных данных, несут ответственность за недопущение пребывания в помещении работников учреждения, не имеющих права доступа в данное помещение, и посторонних лиц в отсутствие лиц, имеющих право доступа в данное помещение.

12.7. Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится комиссией по защите персональных данных и конфиденциальной информации.

13. Ответственность

Сотрудники учреждения, допустившие нарушение правил защиты и использования персональных данных или совершившие действия, приведшие к нарушению целостности данных или к утечке информации, привлекаются к ответственности в соответствии с законодательством Российской Федерации.

Допущенные к персональным данным, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

14. Перечень должностей работников учреждения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

Руководитель учреждения
Заместитель руководителя учреждения
Отдел бухгалтерского учета и отчетности
Начальник отдела
Заместитель начальника отдела
Главный экономист
Ведущий экономист
Отдел правовой, кадровой и административной работы
Начальник отдела

	Главный специалист
	Программист 1 категории
	Специалист 1 категории
Отдел по предоставлению дополнительных мер социальной поддержки	
	Начальник отдела
	Заместитель начальника отдела
	Главный специалист
	Специалист 1 категории
Отдел консультирования и приема документов	
	Начальник отдела
	Заместитель начальника отдела
	Специалист 1 категории
	Специалист 2 категории

14. Перечень приложений к Положению:

1. Заявка на внесение изменений в списки пользователей.
2. Границы контролируемой зоны.
3. Перечень групп пользователей, участвующих в обработке персональных данных в ИСПДн.
Список лиц и определение полномочий для работы в информационных системах, содержащих персональные данные.
4. Инструкция администратора по информационной безопасности и администратора ИСПДн.
5. Инструкция пользователя при работе с информационной системой персональных данных.
6. Инструкция по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций.
7. Инструкция по организации парольной защиты в ИСПДн.
8. Инструкция пользователя при работе с ресурсами сети Интернет.
9. Инструкция пользователя при работе с электронной почтой.
10. Перечень мероприятий для проведения внутренних проверок режима защиты персональных данных.
11. План резервного копирования информационных ресурсов.
12. Обязательство о неразглашении информации, содержащей персональные данные.

Руководитель учреждения



Т.В. Ефимович