Политика информационной безопасности в ГКУ Пензенской области «Ресурсный центр социального обслуживания населения Пензенской области»

1. Общие положения

1.1. Настоящая политика информационной безопасности (далее - Политика) в ГКУ Пензенской области «Ресурсный центр социального обслуживания населения Пензенской области» утверждается директором Центра и определяет мероприятия, процедуры и правила по защите информации в информационных системах Центра

1.2. Положения настоящей Политики распространяются на следующие информационные системы Центра:

- АИС «ЭСРН»;
- ИС «1С бухгалтерия государственного учреждения»;
- ИС «ТОРСЭД».

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей указанных в п. 1.2 информационных систем (далее - Пользователи), а также для системного администратора, администратора баз данных, ответственного за обеспечение безопасности персональных данных в информационных системах Центра (далее - Администраторы).

1.4. Целями настоящей Политики являются:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;
- предотвращение утечек защищаемой информации;
- мониторинг событий безопасности и реагирование на инциденты безопасности;
- нейтрализация актуальных угроз безопасности информации;
- выполнение требований действующего законодательства по защите информации.

1.5. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.6. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утверждённые приказом ФСБ России № 378 от 10.07.2014;

- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. Технологические процессы обработки защищаемой информации в информационных системах

2.1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в информационных системах Центра. Администраторы и Пользователи, допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.

2.1.Технологический процесс обработки персональных данных сотрудников Центра:

2.2.1 Персональные данные следует получать непосредственно у субъекта, либо у законного представителя.

2.2.2. Перед началом обработки персональных данных необходимо получить у субъекта или его законного представителя согласие на обработку персональных данных в письменной форме, в соответствии с утвержденной в Центре формой такого Согласия.

2.2.3. Комплекс документов, сопровождающий процесс оформления трудовых отношений при приёме, переводе и увольнении:

- Информация, представляемая сотрудником при поступлении на работу, должна иметь документальную форму. При заключении трудового договора в соответствии со ст. 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:

- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или сотрудник поступает на работу на условиях совместительства, либо трудовая книжка у сотрудника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета – для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний – при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у сотрудника),

а также лицо, поступающее на работу, предъявляет работодателю:

- свидетельство о заключении брака;
- свидетельство о рождении ребенка;
- фотографию;
- заявление на медицинский полис;
- анкету;
- автобиографию;
- удостоверения, награды, медали;
- сертификаты о повышении квалификации, прохождении курсов, тренингов;
- водительское удостоверение;
- сведения о лицевом счете в банке;

при оформлении сотрудника в Центре специалистом по кадровой работе заполняется унифицированная форма Т-2 «Личная карточка работника».

2.2.Технологический процесс обработки персональных данных при оформлении гражданско-правовых отношений:

2.3.1. Комплекс документов, сопровождающий процесс оформления гражданско-правовых отношений:

- Граждане с целью заключения гражданско-правового договора предъявляют паспортные данные,
- банковские реквизиты ;
- контактные данные;
- свидетельство о присвоении ИНН (при его наличии у сотрудника).

2.3.Технологический процесс обработки персональных данных Заявители, подавшие в Центр заявление о признании нуждающимся в предоставлении социального обслуживания:

2.3.1. Перед началом обработки персональных данных необходимо получить у субъекта или его законного представителя согласие на обработку персональных данных в письменной форме, в соответствии с утвержденной в Центре формой такого Согласия.

2.3.2. Персональные данные заявителей подлежащих обработке:

- фамилия, имя, отчество; дата, место рождения; адрес регистрации или фактического жительства;
- семейное положение (сведения о заключении брака, о расторжении брака, сведения о рождении);
- состав семьи;
- инн, снилс, номер телефона,
- паспортные данные,
- информация о доходах;
- сведения из налоговых деклараций, представленных индивидуальными предпринимателями, применяющими специальные налоговые режимы (ИП);
- сведения о выплатах, произведенных плательщиками страховых взносов в пользу физических лиц;
- сведения о доходах физических лиц по справкам 2-НДФЛ;
- сведения о доходах физических лиц, выплаченных налоговыми агентами;
- сведения о доходах физических лиц из налоговой декларации формы 3-НДФЛ;
- сведения о выплате пособий работающим гражданам в субъектах РФ, участвующих в пилотном проекте ФСС «Прямые выплаты» v.1.0.1(Больничный лист, до 1,5 лет);
- категория получателей социальных услуг,
- группа инвалидности при наличии: сведения медико – социальной экспертизы (МСЭ),
- индивидуальная программа инвалида (ИПРА);
- сведения о жилищно- бытовых условиях при составлении акта обследования условий жизнедеятельности гражданина;
- информация о состоянии здоровья (предоставляется исключительно во исполнении требований действующего законодательства: Федерального закона от 28.12.2013 № 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации», постановлений Правительства Пензенской области: от 15.07.2015 № 399 «Об утверждении порядка предоставления социальных услуг поставщиками социальных услуг в стационарной форме социального обслуживания в Пензенской области»; от 10.11.2015 № 625-пП «Об утверждении Порядка предоставления социальных услуг в форме социального обслуживания на дому в Пензенской области»; от 26.01.2016 № 37-пП «Об утверждении Порядка предоставления поставщиками социальных услуг в полустационарной форме социального обслуживания в Пензенской области», приказа Министерства труда и социальной защиты Российской

Федерации от 29.12.2021 № 929 «О реализации в отдельных субъектах Российской Федерации в 2022 году Типовой модели системы долговременного ухода за гражданами пожилого возраста и инвалидами, нуждающимися в уходе», приказа Министерства труда, социальной защиты и демографии Пензенской области от 18.03.2022 № 145-ОС «Об утверждении Порядка признания граждан нуждающимися в **социальном** обслуживании и их включения в **систему** долговременного ухода".).

2.4.3. Обработка Оператором биометрических персональных данных (сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность) осуществляется в соответствии с законодательством Российской Федерации.

2.4.4. Оператором не осуществляется обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, за исключением случаев, предусмотренных законодательством РФ.

3. Правила и процедуры идентификации и аутентификации пользователей ИС, политика разграничения доступа к ресурсам ИС

3.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику Центра, допущенному к работе с информационными ресурсами Центра присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в информационных системах (далее ИС).

3.2. информационной системе в домене Active Directory.

3.3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ИС запрещено.

3.4. Для администратора безопасности ИС, для системных администраторов ИС, для удаленных пользователей (пользователей работающих с ресурсами ИС через внешние телекоммуникационные сети, но являющихся сотрудниками Центра, для внешних пользователей ИС (пользователей, не под учетной записью Пользователя понимается учетная запись для доступа к являющихся сотрудниками ИС) предусмотрена двухфакторная аутентификация в ИС. Двухфакторная аутентификация подразумевает под собой обязательное выполнение двух факторов: предъявление физического электронного ключа RuToken и ввод пароля (пин-кода) доступа к памяти электронного ключа. Электронные ключи и пароли доступа выдаются Администратором в соответствии с теми же требованиями и правилами, установленными для выдачи учетных записей и паролей к ним в данном разделе настоящей Политики. Идентификация электронного ключа и считывание аутентификационной информации с него осуществляется с помощью механизмов средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД).

3.5. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) пользователя ИС для сотрудника Центра, и предоставления ему (или изменения его) прав доступа к ресурсам ИС инициируется заявкой руководителя подразделения, в котором работает этот сотрудник.

3.6. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики.

3.7. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД и формирует учетную запись, персональный идентификатор и первичный пароль.

Дает ознакомиться с инструкцией Пользователя ИС под роспись, сообщает пользователю идентификационные данные и допускает к работе в ИС.

После допуска к работе в ИС, Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя ИС.

3.8. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе ИС, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИС при разборе инцидентов безопасности.

3.9. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети Центра на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

3.10. Пользователям запрещены любые действия в ИС до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в ИС в ряде случаев. Условия, при которых разрешаются такие действия и перечень разрешенных действий для Администратора до прохождения процедуры идентификации и аутентификации в ИС перечислены в пункте 5.9 инструкции Администратора.

4. Правила и процедуры резервирования технических средств, программного обеспечения, баз данных, средств защиты информации и их восстановления при возникновении нештатных ситуаций

4.1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ИС осуществляется системным администратором Центра.

4.2. Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ИС.

4.3. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

4.4. Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками Центра, имеющими к ней право доступа, в том числе:
  - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  - передача информации по незащищенным каналам связи;
  - обработка информации на незащищенных технических средствах обработки информации;
  - опубликование информации в открытой печати и других средствах массовой информации;
  - передача носителя информации лицу, не имеющему права доступа к ней;
  - утрата носителя с информацией.
- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение информации;
- несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
- несанкционированное подключение технических средств к средствам и системам ИС;
- использование закладочных устройств;
- использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ИС;
- использование злоумышленником уязвимостей программного обеспечения ИС;
- использование злоумышленником программных закладок;
- заражение ИС злоумышленником программными вирусами;
- хищение носителей информации;
- нарушение функционирования технических средств обработки информации;
- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- дефекты, сбои, отказы, аварии технических средств и систем ИС;
- дефекты, сбои, отказы программного обеспечения ИС;
- сбои, отказы и аварии систем обеспечения ИС;
- природные явления, стихийные бедствия:
- термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
- механические факторы (повреждения зданий, землетрясения и т. д.);
- электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

4.5. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, ответственным за информационную безопасность в Центре вырабатывается конкретный план действий с учетом текущей ситуации.

4.6. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

4.7. Инциденты безопасности информации также являются нештатной ситуацией.

4.8. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ИС а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

4.9. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;

- Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
- **в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.**