

УТВЕРЖДЕНО
приказом директора МБУ «КЦСОН «Добрыня»
от «27» апреля 2023 г. № 14

ПОЛОЖЕНИЕ
о конфиденциальной информации в муниципальном бюджетном учреждении
«Комплексный центр социального обслуживания населения «Добрыня»

1. Общие положения

1.1. Настоящее Положение о конфиденциальной информации в муниципальном бюджетном учреждении «Комплексный центр социального обслуживания населения «Добрыня» (далее – Положение) устанавливает общие нормы о сведениях, относящихся к категории конфиденциальных, порядке организации и проведения работ по обработке и защите конфиденциальной информации, определяет единый для всех работников муниципального бюджетного учреждения «Комплексный центр социального обслуживания населения «Добрыня» (далее МБУ «КЦСОН «Добрыня») порядок работы со сведениями конфиденциального характера, порядок допуска к этим сведениям, а также меры ответственности, применяемые за нарушение требований, установленных настоящим Положением.

1.2. Настоящее Положение разработано на основе действующего законодательства Российской Федерации, в том числе Гражданского, Трудового и Уголовного кодексов Российской Федерации и Федерального закона Российской Федерации от 27.07.1997 № 149 «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», а также Указа Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера» и других законодательных и нормативно-правовых актов, регулирующих вопросы охраны конфиденциальной информации.

1.3. Положение распространяется на сведения конфиденциального характера МБУ «КЦСОН «Добрыня» независимо от вида носителя, на котором они зафиксированы.

1.4. Действие настоящего Положения распространяется на работников, заключивших трудовой договор с МБУ «КЦСОН «Добрыня», а также на лиц, работающих по гражданско-правовым договорам, заключенным с МБУ «КЦСОН «Добрыня», которые дали обязательство о неразглашении конфиденциальной информации, в порядке и на условиях, предусмотренных настоящим Положением.

2. Перечень используемых определений, обозначений и сокращений

НСД – несанкционированное действие.

КИ - конфиденциальная информация.

Допуск к КИ – процедура оформления права работника МБУ «КЦСОН «Добрыня» для ознакомления со сведениями, относящимися к конфиденциальным.

Доступ к КИ – ознакомление определенных лиц с КИ с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Защита КИ – деятельность, направленная на предотвращение НСД к КИ и (или) её утечки.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Контрагент – сторона гражданско-правового договора, которой обладатель КИ передал эту информацию.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Обладатель конфиденциальной информации – лицо (физическое или юридическое), которое владеет сведениями, отнесенным к конфиденциальным, на законном основании, ограничило доступ к ним и установило в отношении ее режим конфиденциальности.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных. Общедоступная информация – общеизвестные сведения и иная информация, доступ к которой не ограничен.

Передача конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление конфиденциальной информации – передача сведений, отнесенных к конфиденциальным, и зафиксированных на материальном носителе, ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение конфиденциальной информации – действие или бездействие, в результате которых сведения, отнесенные к конфиденциальным, в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети.

3. Сведения, относимые к конфиденциальным

3.1. Отнесение информации к конфиденциальной осуществляется в порядке, установленном Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера».

К сведениям конфиденциального характера относятся:

- информация, необходимая работодателю в связи с трудовыми, гражданско-правовыми отношениями, касающимися конкретного работника в соответствии с трудовым законодательством Российской Федерации,
- сведения, формируемые для передачи третьим лицам;
- сведения, содержащиеся в договорах (контрактах), заключаемых МБУ «КЦСОН «Добрыня»;
- бухгалтерские документы;
- итоговые (сводные) материалы результатов проверок;

- сведения о порядке и состоянии защиты конфиденциальной информации;
- сведения о защищаемых информационных ресурсах в локальных сетях МБУ «КЦСОН «Добрыня»;
- информация, содержащаяся в личных делах граждан, получающих услуги МБУ «КЦСОН «Добрыня»;
- документы о рассмотрении обращений граждан;
- другие сведения.

3.2. Законодательством Российской Федерации запрещено относить к информации ограниченного доступа:

- законодательные и другие нормативные акты, устанавливающие правовой статус органов государственной власти, органов местного самоуправления, организаций, общественных объединений, а также права, свободы и обязанности граждан, порядок их реализации;
- документы, содержащие информацию о чрезвычайных ситуациях, экологическую, метеорологическую, демографическую, санитарно-эпидемиологическую и другую информацию, необходимую для обеспечения безопасного функционирования населенных пунктов, производственных объектов, безопасности граждан и населения в целом;
- документы, содержащие информацию о деятельности органов государственной власти и органов местного самоуправления, об использовании бюджетных средств и других государственных и местных ресурсов, о состоянии экономики и потребностях населения, за исключением сведений, отнесенных к государственной тайне;
- документы, накапливаемые в открытых фондах библиотек и архивов, информационных системах органов государственной власти области, органов местного самоуправления, общественных объединений, организаций, представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан.

3.3. Информация конфиденциального характера не может быть использована в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан.

3.4. В случае ликвидации МБУ «КЦСОН «Добрыня» решение о дальнейшем использовании служебной информации ограниченного доступа принимает ликвидационная комиссия.

4. Меры по защите конфиденциальной информации. Ответственность за нарушение конфиденциальной информации

4.1. Должностные лица МБУ «КЦСОН «Добрыня» обязаны принимать меры по защите информации конфиденциального характера.

4.2. Руководитель МБУ «КЦСОН «Добрыня» в пределах своей компетенции определяет:

- порядок подготовки, учета, хранения и уничтожения документов и электронных носителей с конфиденциальной информацией;
- порядок обработки конфиденциальной информации с помощью средств электронно-вычислительной техники;
- порядок передачи информации конфиденциального характера другим органам, организациям, а также между структурными подразделениями МБУ «КЦСОН «Добрыня»;
- категории должностных лиц, уполномоченных относить информацию к разряду ограниченного доступа;
- основные мероприятия защиты конфиденциальной информации.

4.3. При поступлении на работу в МБУ «КЦСОН «Добрыня», работник учреждения предупреждается об ответственности за разглашение сведений конфиденциального характера, ставших ему известными в связи с выполнением им своих служебных обязанностей.

4.4. Допуск к конфиденциальной информации предусматривает в трудовом договоре обязательства работника перед работодателем по нераспространению доверенной конфиденциальной информации.

4.5. Доступ исполнителей (пользователей) к конфиденциальной информации осуществляется в соответствии с разрешительной системой допуска исполнителей к документам и сведениям ограниченного доступа.

4.6. Конфиденциальная информация без санкции соответствующего должностного лица МБУ «КЦСОН «Добрыня» не подлежит разглашению (распространению).

4.7. В случае разглашения сведений конфиденциального характера, ставших известными работнику в связи с исполнением им трудовых обязанностей, трудовой договор с работником может быть расторгнут по инициативе работодателя в соответствии с трудовым законодательством.

4.8. Собираение сведений, составляющих конфиденциальную информацию, путем похищения документов, подкупа или угроз, а равно иным незаконным способом влечет уголовную ответственность в соответствии с законом.

4.9. Разглашение конфиденциальной информации (за исключением случаев, когда разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей, влечет дисциплинарную и (или) материальную ответственность.

4.10. Ответственность в соответствии с действующим законодательством несут также работники и должностные лица МБУ «КЦСОН «Добрыня», не выполнившие или не обеспечившие выполнение требований настоящего Положения и тем самым способствовавшие нарушению, а также не принимавшие необходимых и достаточных мер по пресечению ставших им известными фактов нарушения прав МБУ «КЦСОН «Добрыня».

5. Порядок обращения с документами и электронными носителями информации, содержащими конфиденциальную информацию

5.1. Конфиденциальная информация, содержащаяся в документах, имеющих обращение в МБУ «КЦСОН «Добрыня», является служебной информацией ограниченного доступа.

5.2. Прием и учет (регистрация) документов, содержащих информацию конфиденциального характера, осуществляется специалистом МБУ «КЦСОН «Добрыня», которому поручен прием и учет несекретной документации.

5.3. О фактах утраты документов, дел и изданий, содержащих конфиденциальную информацию, либо разглашения этой информации ставится в известность руководитель МБУ «КЦСОН «Добрыня», который назначает комиссию для расследования обстоятельств утраты или разглашения.

Результаты расследования докладываются руководителю, назначившему комиссию.

6. Порядок обмена информацией конфиденциального характера

6.1. Информация конфиденциального характера не подлежит распространению (передаче) без санкции руководителя МБУ «КЦСОН «Добрыня».

6.2. Документированная информация конфиденциального характера, сформированная в процессе деятельности МБУ «КЦСОН «Добрыня» предоставляется органам государственной власти, государственным учреждениям, предприятиям, органам местного самоуправления на безвозмездной основе на основании запроса.

6.3. Передача указанной выше конфиденциальной информации иным пользователям, если иное не установлено законодательством, должна регулироваться договорными отношениями, предусматривающими обязательства и ответственность сторон, перечень сведений, являющихся конфиденциальными и компенсацию за нарушение договорных обязательств.

7. Организация и проведение работ по защите конфиденциальной информации

7.1. Защита конфиденциальной информации осуществляется путем выполнения комплекса мероприятий (правовых, организационных, технических) по предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней, предупреждению преднамеренных программно-технических воздействий с целью разрушения (уничтожения) или искажения информации в процессе обработки, передачи и хранения, по противодействию иностранным техническим разведкам, а также путем проведения специальных работ, порядок организации и выполнения которых определяется Правительством Российской Федерации и федеральными органами исполнительной власти, уполномоченными в области обеспечения безопасности, противодействия техническим разведкам и технической защиты информации, в пределах их полномочий.

7.2. Организация работ по защите конфиденциальной информации возлагается на руководителя МБУ «КЦСОН «Добрыня», руководителей структурных подразделений МБУ «КЦСОН «Добрыня», осуществляющих эксплуатацию объектов информатизации, а методическое руководство и контроль за эффективностью предусмотренных мер защиты информации - на администратора безопасности информации МБУ «КЦСОН «Добрыня», а в случае его отсутствия, на нештатного ответственного за безопасность информации, назначаемого из числа наиболее подготовленных работников.

7.3. Лица, осуществляющие обработку информации конфиденциального характера на средствах вычислительной техники (далее - СВТ), несут ответственность за несоблюдение ими порядка обращения с конфиденциальной информацией.

7.4. В МБУ «КЦСОН «Добрыня» разрабатываются нормативные правовые акты по организации защиты информации.

7.5. При необходимости состав проводимых мероприятий по защите информации может быть дополнен в соответствии с решаемыми задачами и конкретными условиями применения СВТ.

7.6. Для обработки конфиденциальной информации необходимо использовать СВТ в защищенном исполнении с применением сертифицированных программных, технических и программно-технических средств защиты информации. Вычислительные комплексы обработки информации должны быть аттестованы по требованиям безопасности информации. Применяемое программное обеспечение - лицензионным.

7.7. Для передачи конфиденциальной информации по линиям связи, выходящим за пределы контролируемой зоны МБУ «КЦСОН «Добрыня», необходимо использовать защищенные каналы связи (средства криптографической защиты информации).