МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«КОМПЛЕКСНЫЙ ЦЕНТР
СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ»
КРАПИВИНСКОГО
МУНИЦИПАЛЬНОГО ОКРУГА

П Р И К А З

от 06.02.2025 № 19-О
пгт. Крапивинский

Об утверждении Политики
информационной безопасности

В целях обеспечения информационной безопасности в соответствии с требованиями Конституции Российской Федерации, Трудовым кодексом Российской Федерации, Гражданским кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152 «О персональных данных», Федеральным законом 27 июля 2006 года №149 «Об информации, информационных технологиях и о защите информации», а также внутренними нормативными документами КЦСОН Крапивинского округа,

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Политику информационной безопасности муниципального бюджетного учреждения «Комплексный центр социального обслуживания населения» Крапивинского муниципального округа (Приложение № 1);

2. Специалисту по кадрам Цуп М.Ю. ознакомить работников КЦСОН Крапивинского округа с настоящим приказом.

3. Контроль исполнения настоящего приказа оставляю за собой.

4. Настоящий приказ вступает в силу со дня подписания.

Директор КЦСОН Крапивинского округа А.И. Павлова

Приложение № 1
к приказу КЦСОН Крапивинского округа
от 06.02.2025 № 19-О

Политика информационной безопасности Муниципального бюджетного учреждения «Комплексный центр социального обслуживания населения» Крапивинского муниципального округа

1. Общие положения

1.1. Настоящая Политика информационной безопасности разработана в соответствии с положениями:

- Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации";
- Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";
- Федерального закона от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";
- постановления Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";
- приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

1.2. Настоящая Политика информационной безопасности представляет собой совокупность положений, правил и требований, определяющих структуру, необходимый уровень и способы защиты информации, принимаемой, передаваемой, обрабатываемой и хранимой информационной системой КЦСОН Крапивинского округа (далее - информационная система).

Информационная система - это система, построенная на базе компьютерной техники, предназначенная для хранения, поиска, обработки и передачи информации, имеющая определённую практическую сферу применения.

1.3. Защите подлежит вся информация, принимаемая, передаваемая, обрабатываемая и хранимая информационной системой, в том числе содержащая:

- сведения, составляющие служебную и коммерческую тайну, доступ к которым ограничен КЦСОН Крапивинского округа, как собственником информации, в соответствии с положениями предоставленными Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и Федеральным законом от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне";
- персональные данные, доступ к которым ограничен в соответствии с положениями Федерального закона от 27 июля 2006 г. N 152-ФЗ "О персональных данных";
- открытые сведения, в части обеспечения доступности и целостности информации.

1.4. Основными целями Политики информационной безопасности КЦСОН Крапивинского округа являются:

- обеспечение управления и поддержки руководством КЦСОН Крапивинского округа информационной безопасности в соответствии с требованиями учреждения, соответствующими законами и нормами;

- защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба;

- обеспечение целостности и конфиденциальности информации;

- обеспечение соблюдения требований законодательства, руководящих и нормативных документов и общей политики безопасности.

1.4.1. Информационная система обрабатывает персональные данные исключительно в следующих целях:

– принятие решения о возможности заключения трудового договора с кандидатами;

– осуществление трудовых взаимоотношений;

– ведение кадрового учета;

– ведение бухгалтерского учета;

– выплата заработной платы;

– оказании социальных услуг гражданам;

– обучение (повышение квалификации) и должностной рост;

– исполнение должностных обязанностей сотрудниками учреждения;

– учет результатов исполнения должностных обязанностей;

– оформления гражданско-правовых отношений;

– выполнение других функций, возлагаемых на КЦСОН Крапивинского округа законодательством Российской Федерации, Министерством труда и социальной защиты Кузбасса.

1.4.2. Действие настоящей Политики не распространяется на отношения, возникающие при организации хранения, комплектования, учета и использования содержащих персональные данные архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

1.5. Основными задачами Политики информационной безопасности КЦСОН Крапивинского округа являются:

- доступность обрабатываемой информации;

- защита информации от несанкционированного доступа к ней посторонних лиц, от утечки по техническим каналам, от специальных воздействий на информацию в целях её блокирования, уничтожения, искажения;

- контроль целостности и аутентичности (подтверждение авторства) информации, хранимой, обрабатываемой и передаваемой по каналам связи КЦСОН Крапивинского округа;

- обеспечение конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи КЦСОН Крапивинского округа;

- оценка рисков информационной безопасности.

2. Субъекты правоотношений, связанных с использованием информационной системы и обеспечением безопасности информации

2.1. К субъектам правоотношений, связанных с использованием информационной системы и обеспечением безопасности информации относятся:

- КЦСОН Крапивинского округа, как обладатель информации;

- работники КЦСОН Крапивинского округа, как пользователи информационной системой в соответствии с возложенными на них трудовыми обязанностями;

- подразделения КЦСОН Крапивинского округа, обеспечивающие эксплуатацию информационной системы;

- граждане, работающие по договорам гражданско-правового характера;

- иные пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в информационной системе.

2.2. Доступ к информационной системе имеют следующие работники:

- работники КЦСОН Крапивинского округа в соответствии с возложенными на них трудовыми обязанностями.

Уровень доступа к информационной системе определяется для каждого работника индивидуально с соблюдением следующих требований:

- каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;

- конфиденциальная и открытая информация КЦСОН Крапивинского округа размещается на разных серверах;

- непосредственный руководитель работника имеет право на просмотр информации, используемой работником.

Работники КЦСОН Крапивинского округа, как пользователи информационной системой в соответствии с возложенными на них трудовыми обязанностями, обязаны соблюдать следующие требования:

- обрабатывать персональные данные только в рамках закона и с соблюдением принципов, установленных законодательством;

- обеспечивать защиту персональных данных от несанкционированного доступа, уничтожения, модификации или блокирования;

- получать согласие субъектов персональных данных на обработку, если это необходимо по закону;

- не допускать распространения персональных данных без согласия субъектов, если это не предусмотрено законом;

- не допускать несанкционированного доступа к информационной системе;

- использовать информационную систему только для выполнения своих трудовых обязанностей;

- сообщать о всех случаях нарушения безопасности или подозрительных действиях в системе;

- не загружать в систему вредоносное программное обеспечение;

- не пытаться обойти системы защиты;

- соблюдать правила хранения и архивирования данных;

- обеспечить надежную парольную защиту рабочего компьютера, используемых программ для предотвращения несанкционированного доступа к данным.

Все работники должны быть ознакомлены персонально под роспись с организационно-распорядительными документами по защите информации, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению безопасности информации.

Каждый работник при приеме на работу подписывает обязательство о соблюдении требований работы с информационной системой.

Все работники, допущенные к работе с информационной системой несут персональную ответственность за нарушение правил использования, передачи, хранения информации, в том числе конфиденциальной информации.

3. Требования к организации защиты информации, содержащейся в информационной системе

3.1. В информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства

вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

3.2. Для обеспечения защиты информации, содержащейся в информационной системе, КЦСОН Крапивинского округа назначается должностное лицо (работник), ответственные за защиту информации.

3.3. Для проведения работ по защите информации в ходе создания и эксплуатации информационной системы КЦСОН Крапивинского округа в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности".

3.4. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании".

3.5. Защита информации, содержащейся в информационной системе, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной системе, в рамках системы (подсистемы) защиты информации информационной системы (далее - система защиты информации информационной системы).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

- неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

- неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

- неправомерного блокирования информации (обеспечение доступности информации).

3.6. Для обеспечения защиты информации, содержащейся в информационной системе, проводятся следующие мероприятия:

- формирование требований к защите информации, содержащейся в информационной системе;

- разработка системы защиты информации информационной системы;

- внедрение системы защиты информации информационной системы;

- обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы;

- обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

4. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации

4.1. Обеспечение защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации осуществляется КЦСОН Крапивинского округа в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

- архивирование информации, содержащейся в информационной системе;
- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

4.2. Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности КЦСОН Крапивинского округа.

4.3. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

4.4. При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

5. Требования к мерам защиты информации, содержащейся в информационной системе

5.1. Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик информационной системы должны обеспечивать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

5.2. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

5.3. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

5.4. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

5.5. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

5.6. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

5.7. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

5.8. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

5.9. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

5.10. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

5.11. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

5.12. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

5.13. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

5.14. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

6. Обеспечение информационной безопасности персональных данных

6.1. Защита, хранение, обработка и передача персональных данных работников и пользователей информационной системой регламентируется Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных", постановлением Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

6.2. Персональные данные работника - информация, необходимая КЦСОН Крапивинского округа в связи с трудовыми отношениями и касающаяся конкретного работника.

6.3. К персональным данным работника относятся:

- фамилия, имя, отчество;
- пол;
- дата и место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- сведения об образовании, в том числе данные об организациях, осуществляющих образовательную деятельность по реализации профессиональных образовательных программ, о документах об образовании и (или) о квалификации, о договоре о целевом обучении, а также данные о сертификате специалиста или о прохождении аккредитации специалиста;
- иные сведения, необходимые КЦСОН Крапивинского округа в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

6.4. К персональным данным иных пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в информационной системе относятся:

- фамилия, имя, отчество;
- пол;
- дата и место рождения;

- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- история болезни;
- иные сведения, необходимые КЦСОН Крапивинского округа в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

6.5. Все персональные сведения о работниках и иных пользователях КЦСОН Крапивинского округа может получить только от них самих. В случаях когда КЦСОН Крапивинского округа получает необходимые персональные данные работников и иных пользователей только у третьего лица, КЦСОН Крапивинского округа уведомляет об этом работников и иных пользователей и получает от них письменное согласие.

6.6. КЦСОН Крапивинского округа сообщает работникам и иным пользователям о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работников и пользователей дать письменное согласие на их получение.

6.7. Персональные данные работников и иных пользователей являются конфиденциальной информацией и не могут быть использованы КЦСОН Крапивинского округа или любым иным лицом в личных целях.

6.8. При определении объема и содержания персональных данных работников и иных пользователей КЦСОН Крапивинского округа руководствуется настоящим положением, Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, иными федеральными законами.

6.9. Работники и иные пользователи не должны отказываться от своих прав на сохранение и защиту тайны.

6.10. КЦСОН Крапивинского округа принимает организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах, предусмотренные Приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

6.11. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных КЦСОН Крапивинского округа осуществляет блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

6.12. В случае выявления неточных персональных данных при обращении субъекта персональных данных КЦСОН Крапивинского округа осуществляет блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

6.13. В случае подтверждения факта неточности персональных данных КЦСОН Крапивинского округа на основании сведений, представленных субъектом персональных данных, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

6.14. В случае если обеспечить правомерность обработки персональных данных невозможно, КЦСОН Крапивинского округа в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает

такие персональные данные.

6.15. Об устранении допущенных нарушений или об уничтожении персональных данных КЦСОН Крапивинского округа уведомляет субъекта персональных данных.

6.16. В случае достижения цели обработки персональных данных КЦСОН Крапивинского округа прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

6.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных КЦСОН Крапивинского округа прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

6.18. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.15, 6.16. настоящей Политики информационной безопасности, КЦСОН Крапивинского округа осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем: шесть месяцев, если иной срок не установлен федеральными законами.

6.19. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном Федеральными законами.

6.20. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

7. Заключительные положения

7.1. Политика информационной безопасности утверждается руководителем КЦСОН Крапивинского округа и доводится до сведения всех работников КЦСОН Крапивинского округа.

7.2. Основные положения и требования настоящей Политики информационной безопасности распространяются на все структурные подразделения КЦСОН Крапивинского округа.

7.3. Настоящая Политика информационной безопасности вступает в силу с момента ее утверждения.