Приложение 1

к Постановлению администрации
сельского поселения «Слудка»
от 29.08.2014г № 8/43

ИНСТРУКЦИЯ
пользователя по работе с персональными данными

1. Общие положения

1.1 Настоящая Инструкция определяет общие правила работы с персональными данными работников администрации СП «Слудка».
1.2 Пользователь, участвующий в рамках своих функциональных обязанностей в процессах обработки (автоматизированной, без использования средств автоматизации) персональных данных и имеющие доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты.
1.3 Пользователь в своей работе руководствуется настоящей Инструкцией, Положением о персональных данных и другими документами Администрации, регламентирующих организацию обработки персональных данных.
1.4 Методическое руководство работой пользователя осуществляет ответственный за организацию обработки персональных данных.

2. Термины и определения

2.1 Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (в том числе служебная информация ограниченного распространения и персональные данные).
2.2 Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
2.3 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.
2.4 Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.
2.5 Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. В настоящей Инструкции под информационной также подразумевается автоматизированная система и информационная система персональных данных.
2.6 Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

2.7 Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.8 Автоматизированное рабочее место (АРМ) – программно-технический комплекс, посредством которого пользователь выполняет свои должностные обязанности (персональный компьютер, ноутбук, терминал и т.п.).

2.9 Несанкционированный доступ (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

2.10 Посторонние лица – лица, которые не имеют права самостоятельного доступа в помещение и (или) не имеют права самостоятельного доступа в ИС и (или) не имеют допуска к персональным данным.

2.11 Средство защиты информации от несанкционированного доступа (СЗИ НСД) – программное, техническое или программно-техническое средство, направленное на предотвращение или существенное затруднение несанкционированного доступа к информации.

3. Обязанности пользователя

3.1 Не разглашать персональные данные, которые будут доверены или станут известны в ходе рабочего процесса во время выполнения должностных (договорных) обязанностей.

3.2 Не сообщать устно или письменно, не передавать в каком либо виде третьим лицам и не раскрывать публично персональные данные без соответствующего разрешения непосредственного руководителя.

3.3 Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции и других внутренних документов, регламентирующих порядок обработки персональных данных.

3.4 Выполнять на АРМ только те процедуры обработки персональных данных, которые определены должностной инструкцией.

3.5 Знать и соблюдать установленные требования по режиму обработки персональных данных, по учету, хранению и пересылке носителей информации, обеспечению безопасности персональных данных.

3.6 Использовать для хранения персональных данных только определенные места хранения и учтенные носители персональных данных.

3.7 Незамедлительно, в кратчайшие сроки, сообщать руководителю структурного подразделения и ответственному за организацию обработки персональных данных об утрате или недостаче носителей информации, ключей от помещений, хранилищ, сейфов, личных печатей и о других фактах, которые могут привести к разглашению информации, содержащей персональные данные, а также о причинах возможной их утечки (несанкционированного доступа);

3.8 При прекращении трудовых отношений (увольнении) все материальные носители, содержащие персональные данные (флеш-накопители, дискеты, компакт-диски, документы, черновики, распечатки на принтерах, кино- и фотоматериалы, модели, промышленные

образцы и пр.), ключи от помещений, хранилищ, сейфов, личные печати передавать ответственному за организацию обработки персональных данных;

3.9 Использовать информационные ресурсы Администрации и переданные в распоряжение технические средства хранения, обработки и передачи информации исключительно для выполнения порученных работ, должностных (договорных) обязанностей.

3.10 Соблюдать требования Инструкции пользователя локально-вычислительной сети (корпоративной сети).

3.11 Пользователи, имеющие выход в Интернет, обязаны соблюдать правила при работе в сетях связи общего пользования и (или) сетях международного информационного обмена.

3.12 Пользователи, работающие с электронной подписью или использующие шифрование, обязаны соблюдать Инструкцию пользователя по обращению со средствами криптографической защиты информации (СКЗИ).

3.13 Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

3.14 Обо всех выявленных нарушениях, связанных с порядком обработки персональных данных, а так же для получений консультаций по вопросам обработки персональных данных, необходимо обращаться к администратору ИС или ответственному за организацию обработки персональных данных.

4. Пользователям запрещается:

4.1 Нарушать установленные в Администрации правила обработки персональных данных.

4.2 Использовать компоненты программного и аппаратного обеспечения Администрации в неслужебных целях.

4.3 Оставлять свое рабочее место без присмотра, предварительно не заблокировав (штатными средствами операционной системы, либо при помощи штатных средств защиты информации от несанкционированного доступа - при их наличии).

4.4 Оставлять без присмотра или неубранными в хранилища (шкаф, сейф) носители или документы, содержащие персональных данных.

4.5 Записывать и хранить персональные данные на неучтенных носителях информации (оптических дисках, гибких магнитных дисках, флеш-накопителях и т.п.).

4.6 Самовольно изменять состав и конфигурацию используемых программных, аппаратных, программно-аппаратных средств, самовольно устанавливать программное обеспечение, отключать/подключать оборудование или изменять режимы его работы.

4.7 Самовольно подключать АРМ или другие средства к ЛВС Администрации, изменять IP-адрес, MAC-адрес и иные настройки сети АРМ.

4.8 Производить действия, направленные на получение несанкционированного доступа к АРМ и серверам, равно как и любым другим узлам ЛВС Администрации или Интернет, в том числе:
а) действия, направленные на нарушение нормального функционирования элементов сети (компьютеров, другого сетевого оборудования или программного обеспечения);
б) установка программного обеспечения, осуществляющего перехват информации (информационных пакетов), адресованной другим пользователям;
в) действия, направленные на получение несанкционированного доступа к информационным ресурсам, в последующем использовании такого доступа;
г) уничтожение, модификация программного обеспечения или данных без согласования с непосредственным руководителем или владельцами этого ресурса;
д) попытки подбора паролей к любым информационным ресурсам методом перебора всех возможных вариантов паролей, либо атак по словарю;
е) умышленные действия по созданию, использованию и распространению вредоносных программ, в том числе направленных на получение несанкционированного доступа к любым информационным и служебным ресурсам (как внутри Администрации так и вне), либо на нарушение целостности и работоспособности этих систем;
ж) действия по сканированию локальной сети с целью определения ее внутренней структуры, списков открытых портов, наличия существующих сервисов и уязвимостей.

4.9 Самовольно изменять параметры средств защиты информации (в том числе и средств антивирусной защиты), а также завершать их работу и (или) самостоятельно их устанавливать.

4.10 Самостоятельно разрабатывать или использовать нерегламентированное (без разрешения непосредственного руководителя (работника отдела общего обеспечения), не относящиеся к выполнению должностных обязанностей) программное обеспечение.

4.11 Разрешать посторонним лицам работать под своей учетной записью в ИС.

4.12 Пересылать персональные данные по каналам связи в открытом виде, в том числе Интернет, по телефону, факсу, электронной почте и т.п. (без использования средств шифрования).

4.13 Получать доступ к персональным данным с рабочих мест, не оборудованными необходимыми средствами защиты информации.

4.14 Получать доступ к сети Интернет любыми способами, кроме как установленными настоящей Инструкцией, например, при помощи несанкционированно установленных на АРМ модемов и т. п.

4.15 Самовольно создавать совместно используемые сетевые ресурсы (папки общего доступа) на своих компьютерах и файловых серверах, несанкционированно удалять или изменять права доступа к ним.

4.16 В случае возникновения любых механических неисправностей в оборудовании осуществлять самостоятельные попытки их устранения.

4.17 Препятствовать должностным лицам при проведении проверок и служебных расследований, связанных с обеспечением безопасности информации.

4.18 Удалять или искажать программы и файлы с персональными данными и иной важной информацией (например, системной, необходимой для функционирования АРМ, ИС).

4.19 Подключать к ЛВС Администрации личные средства вычислительной техники: ноутбуки, карманные компьютеры, смартфоны и т.п., а так же личные носители и накопители информации.

5. Порядок доступа сотрудников в помещения, предназначенные для обработки персональных данных

5.1 Работники имеют доступ в помещения, предназначенные для работы с персональными данными, в рабочее время без ограничений согласно матрице доступа.

5.2 Присутствие других лиц (другие работники Администрации, субъекты персональных данных и т.д.) в данных помещениях допускается в той мере, в какой этого требуют процессы обработки персональных данных, оказания государственных или муниципальных услуг и исполнения своих должностных обязанностей.

5.3 Уборка помещений выполняется обслуживающим персоналом под контролем работников Администрации согласно матрице доступа.

5.4 В нерабочее время помещения должны опечатываться одним из способов:
а) с помощью пломбиратора и проволоки;
б) с помощью пластилина и пломбира под пластилин;
в) с помощью опечатывающего устройства «под нить» и пломбира под пластилин;
г) с помощью штока и пломбира под пластилин.

5.5 Допускается пребывание в помещениях, предназначенных для обработки персональных данных, работников Администрации в нерабочее время согласно матрицы доступа и при обязательной регистрации в журнале выдачи ключей от помещений в выходные и нерабочие дни.

6. Ответственность

6.1 За неисполнение возложенных настоящей Инструкцией функций и требований лицо, имеющее доступ к документам, содержащих персональные данные субъектов персональных данных и имеющего доступ к аппаратным средствам, программному обеспечению, носителям информации и средствам защиты, содержащих персональные данные, несет персональную ответственность в соответствии с действующим законодательством Российской Федерации.