Приложение 4

к приказу Отдела образования

администрации Сусанинского

муниципального района

Костромской области

от 18 января 2016 г. N 10

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям нормативных документов**

**1. Общие положения**

1.1. Настоящие Правила разработаны на основании требований пункта 4 части 1 ст. 18.1 и пункта 1 части 4 ст. 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и п. б ст. 1 Постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных».

1.2. В соответствии с законодательством Оператор ПДн обязан осуществлять внутренний контроль принятых мер, необходимых и достаточных для обеспечения безопасной обработки персональных данных и иной конфиденциальной информации, обрабатываемой в организации.

1.3. Оператор ПДн самостоятельно с учётом штатной структуры Отдела образования, установленного порядка обработки персональных данных (их сбора, хранения, модификации, передачи, распространения и уничтожения), а также параметров автоматизированной информационной системы, в которой обрабатывается конфиденциальная информация, определяет состав и перечень режимных, правовых и технических мер для обеспечения её защиты.

1.4. Мероприятия по осуществлению внутреннего контроля проводятся на плановой основе в соответствии с утверждаемыми заведующей Отделом образования ежегодными планами.

**2. Основные направления внутреннего контроля**

В соответствии с требованиями федерального законодательства, регулирующего сферу обработки персональных данных и иной конфиденциальной информации регулярному контролю подвергаются:

2.1. Исполнение требований обработки персональных данных, установленных внутренними нормативными документами (Правилами, Положениями, Инструкциями, Порядками).

2.2. Контроль соответствия категорий персональных данных, обрабатываемых в Отделе образования, заявленным в Перечне персональных данных утвержденном актом руководителя.

2.3. Соответствие должностей работников, замещение которых предусматривает обработку персональных данных, заявленному в утвержденном актом Заведующего Отделом образования Перечне должностей.

2.4. Выполнение порядка допуска работников Отдела образования к обработке персональных данных и иной конфиденциальной информации с использованием средств автоматизации и без использования таковых.

2.5. Выполнение работниками Отдела образования требований по обеспечению безопасного хранения материальных и электронных носителей персональных данных и доступа к ним посторонних лиц.

2.6. Реализация исполнения требований учётной политики при работе с материальными и электронными носителями.

2.7. Выполнение установленных режимных требований, правил доступа к местам хранения и обработки конфиденциальной информации, в том числе персональных данных.

2.8. Соответствие требований принятых для ИСПДн мер технической защиты требованиям, предусмотренным приказом ФСТЭК РФ от 18.02.2013 г. № 21, в соответствии с актуальными угрозами и определённым уровнем защищенности персональных данных.

2.9. Исполнение порядка ознакомления работников Отдела образования с нормативными документами, регламентирующими безопасную обработку персональных данных;

2.10. Выполнение порядка и сроков обработки поступающих в Отдел образования запросов от субъектов ПДн.

2.11. Проверка соответствия условий и режима обработки персональных данных, внесенных в реестр Операторов ПДн, действительному положению. Внесение, при необходимости, изменений в направленное ранее Уведомление об обработке ПДн.

**3. Порядок осуществления контроля**

3.1. Осуществление мероприятий внутреннего контроля проводится строго в соответствии с установленными в Плане сроками и обязательной отметкой о выполненном мероприятии.

3.2. Контрольные проверки могут осуществляться лицом, ответственным за организацию обработки персональных данных самостоятельно либо с привлечением должностных лиц, имеющих допуск к обработке персональных данных в соответствии с профилем проводимого мероприятия.

3.3. При необходимости по распоряжению руководства организации могут проводиться внеплановые проверки по различным направлениям порядка обработки и защиты персональных данных.

3.4. За нарушение требований действующего законодательства, виновные несут ответственность в соответствии со ст. 24 Федерального закона от 27.07.2006 г. № 152 ФЗ «О персональных данных».