Муниципальное образовательное учреждение

Каменниковская средняя общеобразовательная школа

Утверждены

приказом от 01.09.2014№01-02/31-40

**ПРАВИЛА**

**осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных**

1. **ОБЩИЕ ПОЛОЖЕНИЯ**
   1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных муниципального образовательного учреждения Каменниковской средней общеобразовательной школы (далее - школа) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
   2. Настоящие Правила определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и действуют постоянно.
2. **ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ**
   1. Тематика проверок обработки персональных данных с использованием средств автоматизации:
      1. соответствие полномочий пользователя матрице доступа;
      2. соблюдение пользователями информационных систем персональных данных школы парольной политики;
      3. соблюдение пользователями информационных систем персональных данных школы антивирусной политики;
      4. соблюдение пользователями информационных систем персональных данных школы правил работы со съемными носителями персональных данных;
      5. соблюдение порядка доступа в помещения школы, где расположены элементы информационных систем персональных данных;
      6. соблюдение порядка резервирования баз данных и хранения резервных копий;
      7. соблюдение порядка работы со средствами защиты информации;
      8. знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях;
   2. Тематика проверок обработки персональных данных без использования средств автоматизации:
      1. хранение бумажных носителей с персональными данными;
      2. доступ к бумажным носителям с персональными данными;
      3. доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.
3. **ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК**
   1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям школа организует проведение периодических проверок условий обработки персональных данных (приложение 1).
   2. Проверки осуществляются ответственным за организацию обработки персональных данных (далее - Ответственный) либо комиссией, созданной директором школы.
   3. Внутренние проверки проводятся по необходимости в соответствии с поручением директора школы.
   4. Проверки осуществляются Ответственным либо комиссией непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.
   5. Для каждой проверки составляется Акт проведения внутренней проверки (приложение 2).
   6. При выявлении в ходе проверки нарушений, Ответственным либо Председателем комиссии в Акте делается запись о мероприятиях по устранению нарушений и сроках исполнения.
   7. Акты хранятся у Ответственного или Председателя комиссии в течение текущего года. Уничтожение Актов проводится Ответственным или комиссией самостоятельно в январе следующего за проверочным годом.
   8. О результатах проверки и мерах, необходимых для устранения нарушений, директору школы докладывает Ответственный или Председатель комиссии.

Приложение № 1

**План**

**внутренних проверок условий обработки персональных данных в администрации Выдропужского сельского поселения**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Тема проверки** | **Нормативный документ, предъявляющий требования** | **Срок проведения** | **Исполнитель** |
|  | Соответствие полномочий пользователя правилам обработки персональных данных | Правила обработки персональных данных.  Политика в отношении обработки персональных данных. | ежегодно | Ответственный за организацию обработки ПДн |
|  | Соблюдение пользователями информационных систем персональных данных парольной политики | Положение об обработке персональных данных. | еженедельно | Ответственный за организацию обработки ПДн |
|  | Соблюдение пользователями информационных систем персональных данных антивирусной политики | еженедельно | Ответственный за организацию обработки ПДн |
|  | Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных | Список помещений Администрации, в которых обрабатываются персональные данные и доступ к ним | ежегодно | Ответственный за организацию обработки ПДн |
|  | Соблюдение порядка резервирования баз данных и хранения резервных копий | Положение по защите персональных данных, обрабатываемых в ИСПДн | еженедельно | Ответственный за организацию обработки ПДн |
|  | Соблюдение порядка работы со средствами защиты информации | ежегодно | Ответственный за организацию обработки ПДн |
|  | Знание пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях | ежегодно | Ответственный за организацию обработки ПДн |
|  | Хранение бумажных носителей с персональными данными | Положение об обработке персональных данных без использования средств автоматизации. | ежегодно | Ответственный за организацию обработки ПДн |
|  | Доступ к бумажным носителям с персональными данными | ежегодно | Ответственный за организацию обработки ПДн |
|  | Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными | Положение об обработке персональных данных без использования средств автоматизации.  Список помещений, в которых обрабатываются персональные данные и доступ к ним. | ежегодно | Ответственный за организацию обработки ПДн |

Приложение 2

Муниципальное образовательное учреждение

Каменниковская средняя общеобразовательная школа

УТВЕРЖДАЮ

Директор школы

\_\_\_\_\_\_\_\_\_Н.А.Силанова

«\_\_\_\_»\_\_\_\_\_\_\_\_20\_\_\_г.

АКТ

внутреннего контроля соответствия обработки персональных данных

федеральному закону «О персональных данных»

п.Каменники «\_\_\_»\_\_\_\_\_\_\_\_20\_\_г.

Настоящий акт составлен в том, что \_\_.\_\_.201\_\_г. ответственным за организацию обработки персональных данных или комиссией по внутреннему контролю проведена проверка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(тема проверки)

Проверка осуществлялась в соответствии с требованиями \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(название документа)

В ходе проверки проверено:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Выявленные нарушения:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Меры по устранению нарушений:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Срок устранения нарушений: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Должность ответственного \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ФИО

или

|  |  |
| --- | --- |
| Председатель: | |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (ФИО) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) |
| Члены комиссии: |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (ФИО) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (ФИО) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (ФИО) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) |

Должность руководителя проверяемого

подразделения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ФИО