Приложение №4

к приказу 26/1 от 01.09.2018года

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных в информационной системе персональных данных Муниципального дошкольного образовательного учреждения детский сад №1п.Рамешки**

**Общие положения**

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в информационной системе персональных данных Муниципального дошкольного образовательного учреждения детский сад №1 п.Рамешки (далее Учреждение) разработаны в соответствии с законодательством Российской Федерации и законодательством Тверской области и определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1. **Тематика внутреннего контроля.**

1.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

а) соответствие полномочий пользователя матрице доступа;

б) соблюдение пользователями информационной системы персональных данных (далее ИСПДн) Учреждения требований инструкции по организации парольной защиты в информационных системах персональных данных Учреждения;

в) соблюдение пользователями ИСПДн требований инструкции по организации антивирусной защиты в информационных системах персональных данных Учреждения;

г) соблюдение порядка доступа в помещения Учреждения, в которых ведется обработка персональных данных работников;

д) знание пользователями ИСПДн порядка своих действий во внештатных ситуациях.

1.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

а) соблюдение правил хранения бумажных носителей с персональными данными;

б) соблюдение порядка доступа к бумажным носителям с персональными данными;

в) соблюдение порядка доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

1. **Порядок проведения внутренних проверок.**

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организуется проведение периодических проверок условий обработки персональных данных в соответствии с планом проверок (приложение №1 к Правилам).

2.2. Проверки осуществляются комиссией, создаваемой приказом директора Учреждения.

2.3. Внутренние проверки проводятся по необходимости, в соответствии с поручением директора Учреждения, но не реже одного раза в год.

2.4. Внутренние проверки осуществляются непосредственно на месте обработки персональных данных путем опроса, либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

2.5. По результатам каждой проверки составляется Протокол проведения внутренней проверки (приложение №2 к Правилам).

2.6. При выявлении в ходе проверки нарушений председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.7. Протоколы хранятся у Ответственного в течение текущего года. Уничтожение протоколов проводится Ответственным самостоятельно в первом квартале года, следующего за отчетным.

2.8. О результатах проверки и мерах, необходимых для устранения нарушений, директору Учреждения докладывает председатель комиссии.

Приложение №1

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

УТВЕРЖДАЮ

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

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

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

**План**

**внутренних проверок условий обработки персональных данных**

**в информационной системе персональных данных Муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы №\_\_\_\_\_\_ города** \_\_\_\_\_\_\_\_\_\_\_\_\_\_

| № п/п | Тема проверки | Нормативный документ, предъявляющий требования | Срок проведения | Исполнитель |
| --- | --- | --- | --- | --- |
|  | Соответствие полномочий пользователя требованиям к защите персональных данных | Нормативные документы Учреждения, принятые в соответствии с Постановлением Правительства РФ №211 от 21.03.2012г. |  |  |
|  | Соблюдение пользователями ИСПДн парольной политики | Инструкция по организации парольной защиты в ИСПДн |  |  |
|  | Соблюдение пользователями ИСПДн антивирусной политики | Инструкция по организации антивирусной защиты в ИСПДн |  |  |
|  | Соблюдение порядка доступа в помещения, где расположены элементы ИСПДн | Порядок доступа работников в помещения, где ведется обработка персональных данных |  |  |
|  | Знание пользователями ИСПДн своих действий во внештатных ситуациях | Политика в отношении обработки персональных данных работников |  |  |
|  | Хранение бумажных носителей с персональными данными | Законодательство Российской Федерации |  |  |
|  | Доступ к бумажным носителям с персональными данными | Законодательство Российской Федерации |  |  |

Приложение №2

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

УТВЕРЖДАЮ

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

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

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.

**Протокол**

**проведения внутренней проверки условий обработки**

**персональных данных** **в информационной системе персональных данных Муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы №\_\_\_\_\_\_ города** \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Настоящий Протокол составлен в том, что «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_\_ г. лицом, ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю в составе:

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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Председатель комиссии:

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

(Ф.И.О.) (подпись)

Члены комиссии:

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

(Ф.И.О.) (подпись)

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

(Ф.И.О.) (подпись)

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

(Ф.И.О.) (подпись)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.