|  |  |  |
| --- | --- | --- |
|  |  | УТВЕРЖДАЮДиректор МБУ ДО СШ №4 г. Туапсе МО Туапсинский район\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.А. Забураев"\_\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г. |

**Разрешительная система доступа к персональным данным,
содержащимся в базах данных муниципального**

**бюджетного учреждения дополнительного образования**

**спортивная школа №4**

**г. Туапсе МО Туапсинский район**

**Разработал**

Администратор информационной

безопасности МБУ ДО СШ №4 г.Туапсе

МО Туапсинский район

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.А. Манькова

"\_\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2023г.

г. Туапсе

2023 год

# Общие положения

1.1. Разрешительная система доступа к персональным данным, содержащимся в базах данных является локальным нормативным актом муниципального бюджетного учреждения дополнительного образования спортивная школа №4 г. Туапсе МО Туапсинский район устанавливает правила доступа сотрудников и сторонних организаций к персональным данным, содержащимся в базах данных (далее соответственно – положение, учреждение, персональные данные).

1.2. В настоящем положении используются следующие основные понятия
в соответствии, в том числе с Федеральным законом Российской Федерации
от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

***Персональные данные (ПДн)***– любая информация, относящаяся к прямо
или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

***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.

***Конфиденциальность персональных данных***– обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

***Информационные ресурсы организации, содержащие персональные данные***–отдельные документы и массивы документов, а также документы и массивы документов в информационных системах (банках данных, архивах), доступ к которым ограничен в соответствии с законодательствомРоссийской Федерации и локальными нормативными актами организации, икоторые содержат персональные данные.

***Доступ пользователя к информационным ресурсам***–ознакомление
с информацией, ее обработка, в частности, копирование, модификация
или уничтожение информации.

# Порядок предоставления доступа

2.1. Предоставление доступа сотрудникам к любым информационным ресурсам должно осуществляться только на основании заявок, оформленных
в соответствии приложением 1 к настоящему положению.

2.2. Перед предоставлением сотруднику доступак информационным ресурсамучреждения, содержащим персональные данные, необходимо:

- отразить в трудовом договоре с сотрудником обязательства о неразглашенииперсональных данных, которыебудут ему известны при исполнении служебных обязанностей, и о соблюдении требований локальных нормативных актов, регулирующих порядок обращения с персональными данными;

- ознакомить сотрудника под подпись со следующими документами:

а) переченьперсональных данныхучреждения;

б) инструкция по обеспечению безопасности обрабатываемых персональных данных;

в) инструкции пользователей информационных систем персональных данных (для всех ИСПДн, используемых в учреждении).

2.3. На основании распорядительного актаруководителя учреждения
(при необходимости) осуществляется допуск пользователя к персональным данным, в объеме, необходимомдля выполнения им своих функциональных обязанностей.

2.4. При переводе на другую должность основанием для допуска служит приказ директора, при этом допуск работника по предыдущей должности прекращается, и он допускается к сведениям по новой должности.

2.5. Перечень персональных данныхучреждениянеобходимо поддерживать в актуальном состоянии.

# Порядок получения разрешения на предоставление доступа

3.1. Предоставление пользователям доступа к персональным даннымучрежденияосуществляется следующим образом:

заявка на предоставление доступа к ресурсу, подписанная непосредственным руководителем, направляется ответственному за этот ресурс лицу;

подписанная ответственным за ресурслицом заявка согласовывается
с администратором информационной безопасности и направляется системному администратору для предоставления доступа пользователю к запрашиваемому ресурсу.

3.2. Срок рассмотрения заявки на предоставление доступа пользователей
к информационным ресурсам не должен превышать одного рабочего дня.

# Порядок прекращения доступа

4.1. Прекращение предоставления доступа пользователям к персональным даннымучреждения осуществляется следующим образом:

в случае увольнения (перевода на другую должность) сотрудника заявка
на отключение доступа к ресурсу, подписанная непосредственным руководителем, направляется ответственному за этот ресурс лицу;

подписанная ответственным за ресурс лицом заявка направляется системному администратору и администратору информационной безопасности для отключения доступа пользователя к ресурсу.

4.2. В случае компрометации аутентификационных данных пользователя руководитель подразделения извещает в письменном виде администратора информационной безопасности о факте компрометации.

4.3 Администратор информационной безопасности должен уведомить
в письменном виде ответственного за ресурс и лицо, выполняющее функции системного администратора, о необходимости отключения доступа пользователя к ресурсу и инициировать служебное расследование.

# Контрольдоступак информационным ресурсам

5.1. Контроль правомерности предоставления доступа пользователей
к информационным ресурсам возлагается на администратора информационной безопасности.

# Ответственность

6.1. Сотрудники учреждения, допущенные к работе с персональными данными, несут ответственность за разглашение персональных данных в соответствии с законодательством Российской Федерации.

# Перечень локальных нормативных актов,ознакомление с которыми рекомендуется в целях соблюдения требований настоящего положения

Перечень защищаемой информации вучреждении.

Инструкция пользователя ИСПДн.

Инструкция пользователя ИСПДн на случай возникновения внештатных ситуаций.

Инструкция администратора ИБ.

*Приложение 1*

**Заявка на доступ к информационным ресурсам**

|  |  |
| --- | --- |
| Наименование информационного ресурса |  |
| ФИО сотрудника, получающего доступ |  |
| Права |  |
| Основание получения доступа |  |

Подпись непосредственного руководителя сотрудника, запрашивающего доступ:

Должность\_\_\_\_\_\_\_\_\_\_\_\_\_\_ подпись \_\_\_\_\_\_\_\_\_\_\_\_\_ Инициалы, фамилия

СОГЛАСОВАНО:

Администраторинформационной безопасности

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

 (подпись) (инициалы, фамилия)

Доступ предоставлен:

Администратор ИСПДн

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

 (название ИСПДн) (подпись) (инициалы, фамилия)

**Отметка об ознакомлении пользователя с локальными нормативными актами по информационной безопасности:**

Перечень персональных данных учреждения.

Положение о порядке организации и проведения работ по защите персональных данных учреждения.

Инструкция пользователя

|  |  |
| --- | --- |
| Дата | Подпись |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |