УТВЕРЖДЕНО
Приказом МДОУ ДС «Морошка»
№ 23-ОД от 18.11.2022г.

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в МДОУ ДС «Морошка»

Приложение к приказу **№ 23-ОД** от 18.11.2022

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в МДОУ ДС «Морошка»

1. Общие положения

1.1. Настоящая Инструкция ответственного за обеспечение безопасности персональных данных (далее - Инструкция) определяет основные обязанности, права ответственного лица за обеспечение безопасности персональных данных в МДОУ ДС «Морошка» (далее - МДОУ).

1.2. Ответственный за обеспечение безопасности персональных данных (далее - Ответственный) назначается приказом МДОУ из числа руководителей структурных подразделений МДОУ.

1.3. Ответственный за обеспечение безопасности персональных данных в МДОУ подчиняется ответственному за организацию обработки персональных данных в МДОУ, в части вопросов, касающихся обработки и обеспечения безопасности персональных данных в МДОУ, ему подчиняются администраторы безопасности информации (далее-АБИ) МДОУ.

1.4. Ответственный осуществляет методическое руководство АБИ, сотрудников МДОУ, имеющих санкционированный доступ к персональным данным, в вопросах обеспечения безопасности персональных данных.

1.5. Все сотрудники МДОУ обязаны выполнять требования Ответственного за обеспечение безопасности персональных данных в части вопросов, касающихся обеспечения безопасности персональных данных в МДОУ.

1.6. Ответственный за обеспечение безопасности персональных данных в своей работе руководствуется настоящей Инструкцией, руководящими и нормативными документами ФСТЭК России и муниципальными правовыми актами.

1.7. Ответственный за обеспечение безопасности персональных данных отвечает за качество проводимых им работ по контролю за действиями при работе в информационной системе персональных данных (далее - ИСПД), состояние и поддержание установленного уровня защиты ИСПД.

2. Обязанности Ответственного за обеспечение безопасности персональных данных

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, регламентирующих порядок действий по организации обработки персональных данных.

2.2. Ознакомлять под подпись сотрудников, имеющих доступ к персональным данным, с организационно-распорядительными документами обеспечения безопасности персональных данных МДОУ, и требовать их исполнения.

2.3. Проводить инструктаж и консультации пользователей информационной системы персональных данных по соблюдению режима конфиденциальности.

2.4. Контролировать физическую сохранность средств и оборудования информационной системы персональных данных подразделения.

2.5. Организовывать периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченньми структурами.

2.6. Взаимодействовать с администратором безопасности по вопросам обеспечения и выполнения требований обработки персональныхданных Организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от несанкционированного доступа.

2.7. Контролировать периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации.

2.8. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в ИСПД и по

правилам обработки персональных данных.

2.9. Знать перечень и условия обработки персональных данных в МДОУ.

2.10. Знать перечень установленных в подразделении технических средств, входящих в состав информационных систем, и перечень задач, решаемых с их использованием.

2.11. Обеспечивать соблюдение сотрудниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационных систем.

2.12. Осуществлять контроль за порядком учета, создания, хранения и использования машинных (выходных) документов, содержащих персональные данные.

2.13. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационных систем и осуществления несанкционированного доступа к персональным данным и техническим средствам из состава информационных систем подразделения, сообщать непосредственному руководителю.

2.14. Инструктировать сотрудников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами зашиты информации.

2.15. Знать законодательство РФ о персональных данных, следить за его изменениями.

2.16. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.17. Выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

3. Права ответственного за обеспечение безопасности персональных данных

3.1.Требовать от всех пользователей информационных систем персональных данных подразделения выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных.

3.2. Инициировать блокирование доступа сотрудников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных.

3.3. Участвовать в разработке мероприятий по совершенствованию системы защиты персональных данных.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

3.5. Обращаться с предложением о приостановке процесса обработки персональных данных или отстранении от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности. Подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПД, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

4. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

- сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;
- действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПД, при использовании учетной записи администратора или другого пользователя ИСПД, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

4.2. При выявлении факта несанкционированного доступа Ответственный обязан:

4.2.1. по возможности пресечь дальнейший несанкционированный доступ к персональным данным;

4.2.2. доложить в служебной записке о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

4.2.4. известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного доступа.

5. Ответственность

5.1. Ответственный несет персональную ответственность за:

5.1.1. соблюдение требований настоящей Инструкции;

5.1.2. правильность и объективность принимаемых решений;

5.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных.

5.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.