Департамент образования
Администрации муниципального образования город Салехард
муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад «Мозаика»

Рассмотрено
на общем собрании трудового
коллектива
протокол № 6 от 1 февраля 2022 г.

Утверждено приказом заведующего
МБДОУ Детский сад «Мозаика»
_____ М.А. Байдашина
от № 28 от 2 февраля 2022 г.

Инструкция ответственного за организацию обработки и обеспечение безопасности персональных данных в муниципальном бюджетном дошкольном образовательном учреждении «Детский сад «Мозаика»

1. Общие положения

1.1. Данная Инструкция определяет основные обязанности, права ответственного лица за организацию обработки и обеспечение безопасности персональных данных (ответственного за защиту информации) (далее – Ответственный) муниципального бюджетного дошкольного образовательного учреждения «Детский сад «Мозаика» (далее – Организация).

1.2. Ответственный является штатным работником Организации и назначается приказом руководителя Организации.

1.3. Ответственный отвечает за организацию и состояние процесса обработки информации ограниченного доступа в информационной системе (далее – информационная система), в том числе персональных данных.

1.4. Решение вопросов организации обработки и обеспечения защиты информации, обрабатываемой в информационной системе, входит в прямые трудовые обязанности Ответственного.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, руководящими и нормативными документами ФСТЭК России, а также другими нормативно-правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами Организации.

1.7. Требования Ответственного, связанные с выполнением им своих трудовых обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к защищаемой информации.

1.8. Ответственный обладает правами доступа к любым носителям информации Организации.

2. Термины и определения

2.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.2. Администратор безопасности информации – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системой защиты информации в соответствии с установленной ролью.

2.3. Безопасность информации [данных] – состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность.

2.4. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.5. Доступность информации [ресурсов информационной системы] – состояние информации [ресурсов информационной системы], при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

2.6. Защищаемая информация – информация, для которой обладателем информации определены характеристики ее безопасности.

2.7. Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.8. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.9. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.10. Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2.11. Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

2.12. Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

2.13. 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.

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

2.15. Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования.

2.16. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.17. Средство защиты информации – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты информации.

2.18. Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

3. Обязанности ответственного

Ответственный обязан:

3.1. Обеспечивать выполнение режимных и организационных мероприятий на месте эксплуатации информационной системы, а также следить за выполнением требований по условиям размещения средств вычислительной техники и их сохранностью.

3.2. Знать и предоставлять администратору безопасности информации изменения к списку лиц, доступ которых к информации ограниченного доступа необходим для выполнения трудовых обязанностей.

3.3. Проводить инструктаж и консультации пользователей информационной системы по соблюдению режима конфиденциальности.

3.4. Участвовать в определении полномочий пользователей информационной системы (оформлении разрешительной системы доступа), минимально необходимых им для выполнения трудовых обязанностей.

3.5. 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 уполномоченными структурами.

3.6. Взаимодействовать с администратором безопасности информации по вопросам обеспечения и выполнения требований обработки персональных данных.

3.7. Контролировать осуществление мероприятий по установке и настройке средств защиты.

3.8. Организовывать работы по плановому контролю работоспособности технических средств защиты информации, охраны объекта, средств защиты информации от несанкционированного доступа.

3.9. Контролировать периодическое резервное копирование баз данных и сопутствующей защищаемой информации.

3.10. По указанию руководства своевременно и точно отражать изменения в локальных нормативно-правовых актах по управлению средствами защиты информации в информационной системе и по правилам обработки информации ограниченного доступа.

3.11. Знать перечень и условия обработки персональных данных в Организации.

3.12. Знать перечень установленных в подразделении технических средств, входящих в состав информационной системы, и перечень задач, решаемых с их использованием.

3.13. Обеспечивать соблюдение работниками утвержденного порядка проведения работ по установке и модернизации аппаратных и программных средств компьютеров и серверов из состава информационной системы.

3.14. Осуществлять контроль за порядком учета, создания, хранения и использования машинных (выходных) документов, содержащих защищаемую информацию.

3.15. При выявлении возможных каналов неправомерного вмешательства в процесс функционирования информационной системы и осуществления несанкционированного доступа к защищаемой информации и техническим средствам из состава информационной системы подразделения, сообщать о них руководителю Организации.

3.16. Инструктировать работников по вопросам обеспечения информационной безопасности и правилам работы с применяемыми средствами зашиты информации.

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

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

3.19. Выполнять иные мероприятия, требуемые нормативными документами по защите информации.

4. Права ответственного

Ответственный имеет право:

4.1. Требовать от всех пользователей информационной системы выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности информации.

4.2. Инициировать блокирование доступа работников к защищаемой информации, если это необходимо для предотвращения нарушения режима защиты информации.

4.3. Участвовать в разработке мероприятий по совершенствованию системы защиты информации.

4.4. Инициировать проведение служебных расследований по фактам нарушения

установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей защищаемой информации, нарушения правил работы с документами, содержащими персональные данные, несанкционированного доступа, утраты, порчи защищаемых носителей информации и технических средств из состава информационной

системы или по другим нарушениям, которые могут привести к снижению уровня информационной безопасности.

4.5. Обращаться к руководителю подразделения с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности.

4.6. Подавать свои предложения по совершенствованию мер защиты информации, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня информационной безопасности.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам несанкционированного доступа относятся:

5.1.1. сеансы работы в информационной системе незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к информационной системе, при использовании учетной записи администратора или другого пользователя, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа Ответственный обязан:

5.2.1. по возможности пресечь дальнейший несанкционированный доступ к защищаемой информации;

5.2.2. доложить руководителю Организации служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

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

5.2.4. известить администратора безопасности информации о факте несанкционированного доступа.

6. Ответственность

6.1. Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции;

6.1.2. правильность и объективность принимаемых решений;

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности информации;

6.1.4. за все действия, совершенные от имени его учетной записи в информационной системе, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту информации ограниченного доступа, несет дисциплинарную, административную, гражданско - правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.