Российская Федерация
Ханты – Мансийский автономный округ - Югра
(Тюменская область)
Муниципальное образование Октябрьский район
Управление образования и молодёжной политики администрации Октябрьского района
Муниципальное бюджетное дошкольное образовательное учреждение
«Детский сад общеразвивающего вида «Аленький цветочек»
(МБДОУ «ДСОВ «Аленький цветочек»)
628 109, улица Лесная, 36, с. Перегрёбное, Октябрьский район, Тюменская область, ХМАО – Югра
тел. 8 (34678) 38 637, факс 8 (34678) 38 643, 38 747, e-mail: alcvet-ds@oktregion.ru
ОКПО 57421193 ОГРН 1038600200033 ИНН 8614005936 КПП 861401001

УТВЕРЖДЕНА
Приказом Заведующего
МБДОУ «ДСОВ «Аленький цветочек»
от 16.08.2017 № 533 - од

Регистрационный номер 50 - ор

ПОЛИТИКА
в отношении обработки и защиты персональных данных в Муниципальном бюджетном дошкольном образовательном учреждении «Детский сад общеразвивающего вида «Аленький цветочек»

Подписан: Светлана Николаевна Куделькина
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: 628109, Россия, ХМАО-Югра, Тюменская область, Октябрьский район, с. Перегребное, улица Лесная, дом 36.
Дата: 2021.02.12 11:29:22+05'00'

село Перегрёбное, 2017

1. Общие положения

1.1. Настоящая Политика раскрывает состав субъектов персональных данных, принципы, порядок и условия обработки персональных данных работников и иных лиц, чьи персональные данные обрабатываются в Муниципальном бюджетном дошкольном образовательном учреждении «Детский сад общеразвивающего вида «Аленький цветочек» (далее – Организация, Оператор).

1.2. В целях выполнения норм федерального законодательства в области обработки персональных данных субъектов персональных данных Оператор считает важнейшими своими задачами соблюдение принципов законности, справедливости и конфиденциальности при обработке персональных данных, а также обеспечение безопасности процессов их обработки.

1.3. Политика в отношении обработки и защиты персональных данных в Организации характеризуется следующими признаками:

1.3.1. Раскрывает основные категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки Оператором персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

1.3.2. Является общедоступным документом, декларирующим концептуальные основы деятельности Оператора при обработке персональных данных.

1.4. Политика разработана в соответствии со следующими нормативными документами:

- Конституция Российской Федерации;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.5. Целями Политики являются:

- обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;
- обеспечение защиты от несанкционированного доступа и неправомерного распространения персональных данных, обрабатываемых в информационных системах Организации.

1.6. Основные понятия, используемые в Политике:

- персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация (пункт 1 статья 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также

определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

- обработка персональных данных работника - 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 (пункт 3 статья 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;
- информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
- распространение персональных данных - действия, направленные на раскрытие персональных данных работников неопределенному кругу лиц (пункт 5 статья 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- предоставление персональных данных - действия, направленные на раскрытие персональных данных работников определенному лицу или определенному кругу лиц (пункт 6 статья 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- блокирование персональных данных - временное прекращение обработки персональных данных работников (за исключением случаев, если обработка необходима для уточнения персональных данных) (пункт 7 статья 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных работников и (или) в результате которых уничтожаются материальные носители персональных данных работников (пункт 8 статья 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному работнику (пункт 9 статья 3 Федерального закона от 27.07.2006 № 152-ФЗ);
- информация - сведения (сообщения, данные) независимо от формы их представления;
- документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

1.7. Политика действует в отношении информации, которую Оператор получает о субъекте персональных данных в процессе осуществления своей деятельности, предоставления услуг или исполнения договорных обязательств.

1.8. Персональные данные являются конфиденциальной, строго охраняемой информацией и на них распространяются все требования, установленные внутренними документами Организации по защите конфиденциальной информации.

Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении 75 лет срока их хранения.

1.9. Требования Политики распространяются на всех работников Организации (штатных, временных, работающих по внешнему совместительству и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.), связанных с обработкой персональных данных.

1.10. Настоящая Политика вступает в силу с момента её утверждения приказом руководителем Организации и действует бессрочно, до замены новой Политикой. Все изменения в Политику вносятся приказом. Все работники Организации должны быть ознакомлены с настоящим Положением под личную подпись.
1.11. Политика является общедоступной и подлежит размещению на официальном сайте Организации в сети «Интернет».
1.12. Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.
1.13. Контроль исполнения требований Политики осуществляется ответственным лицом за обеспечение безопасности персональных данных в Организации.

2. Информация об Операторе

2.1. Полное наименование Организации: Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад общеразвивающего вида «Аленький цветочек».
2.2. Сокращенное наименование Организации: МБДОУ «ДСОВ «Аленький цветочек».
2.3. ОГРН 1038600200033 ИНН 8614005936.
2.4. Юридический адрес Оператора: Россия, Тюменская область, Ханты-Мансийский автономный округ - Югра, Октябрьский район, село Перегрёбное, ул. Лесная, д. 36, почтовый индекс 628109.
2.5. Фактический адрес Оператора: Россия, Тюменская область, Ханты-Мансийский автономный округ - Югра, Октябрьский район, село Перегрёбное, ул. Лесная, д. 36, почтовый индекс 628109.
2.6. Телефоны, факс: 8(34678) 38 637 (руководитель), 8(34678) 38747 (ответственный работник).
2.7. Регистрационный номер записи в Реестре операторов, осуществляющих обработку персональных данных: персональных данных: 10-0102169.

3. Цели сбора персональных данных

3.1.Оператор осуществляет обработку персональных данных в следующих целях:

а) заключения, исполнения и прекращения трудовых договоров с физическими лицами и иными лицами, в случаях, предусмотренных действующим законодательством и локальными нормативными актами Организации;

б) организации кадрового учёта, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым договорам; ведения кадрового делопроизводства, содействия сотрудникам в обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных»;

в) оказания образовательной услуги по реализации образовательных программ дошкольного образования, дополнительных образовательных программ по дополнительному образованию по дополнительным программам дошкольного образования;

г) организации работы с обращениями граждан.

4. Принципы и условия обработки персональных данных

4.1. Основной задачей обеспечения безопасности персональных данных при их обработке в Организации является предотвращение несанкционированного доступа к ним третьих лиц, предупреждение преднамеренных программно-технических и иных воздействий с целью хищения персональных данных, разрушения (уничтожения) или искажения их в процессе обработки.

4.2. Обработка персональных данных в Организации осуществляется на основе следующих принципов:

а) законности и справедливости целей и способов обработки персональных данных; соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Организации;

б) соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

в) достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

г) недопустимости объединения, созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

д) хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

е) уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

4.3. Обработка персональных данных осуществляется на основании условий, определенных законодательством Российской Федерации

5. Правовые основания обработки персональных данных

5.1. Правовым основанием обработки персональных данных являются:

- Устав Организации.
- Трудовые договора с работниками Организации.
- Согласие на обработку персональных данных.

6. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных

6.1. В зависимости от субъекта персональных данных Организация обрабатывает персональные данные следующих категорий субъектов персональных данных:

а) персональные данные руководителя Организации, необходимые Организации для выполнения своих обязательств в рамках договорных отношений для выполнения требований законодательства Российской Федерации;

б) персональные данные воспитанников Организации и их родителей (законных представителей);

в) персональные данные работников Организации;

г) граждан, обращающихся в Организацию в соответствии с Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан в Российской Федерации».

6.2. Перечень персональных данных, подлежащих защите Организацией формируется в соответствии с федеральным законодательством о персональных данных и перечнями персональных данных, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с осуществлением деятельности Организации, определенной Уставом.

6.3. Сведениями, составляющими персональные данные, является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

6.4. В состав персональных данных работников Организации входят документы, содержащие информацию о паспортных данных, образовании, отношении к воинской обязанности, семейном положении, месте жительства, состоянии здоровья, а также о предыдущих местах их работы.

6.5. К персональным данным относят данные, которые содержат:

а) индивидуальные данные о конкретном работнике, используемые должностными лицами Организации при исполнении своих должностных обязанностей;

б) индивидуальные данные, предоставляемые Организации родителями (законными представителями) воспитанников и иными лицами в рамках договорных отношений.

6.6. Персональные данные составляют:

а) сведения о фактах, событиях и обстоятельствах частной жизни субъекта персональных данных, позволяющие идентифицировать его, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;

б) служебные сведения, а также иные сведения, связанные с профессиональной деятельностью работника, в том числе сведения о поощрениях и о дисциплинарных взысканиях.

6.7. Персональные данные субъекта могут содержать следующую информацию:

- фамилия, имя, отчество;
- пол, возраст;
- образование, квалификация, профессиональная подготовка и сведения о повышении квалификации;
- состояние здоровья;
- место жительства;
- семейное положение, наличие детей;
- факты биографии и предыдущая трудовая деятельность (место работы, размер заработка, судимость, служба в армии, работа на выборных должностях, на государственной службе и др.);
- финансовое положение (доходы, владение недвижимым имуществом и др.);
- деловые и иные личные качества, которые носят оценочный характер;
- принадлежность лица к конкретной нации, этнической группе, расе;
- биометрические данные;
- прочие сведения, которые могут идентифицировать человека.

6.8. Документами, содержащими персональные данные работника, являются:

- паспорт или иной документ, удостоверяющий личность;
- трудовая книжка;
- страховое свидетельство обязательного пенсионного страхования;
- свидетельство о постановке на учёт в налоговый орган и присвоения ИНН;
- документы воинского учёта;
- документы об образовании, о квалификации или наличии специальных знаний или специальной подготовки;
- автобиография;
- личный листок по учёту кадров;
- медицинское заключение о состоянии здоровья;
- документы, содержащие сведения о заработной плате, доплатах и надбавках;
- трудовой договор;
- приказы о приеме лица на работу, об увольнении, а также о переводе лица на другую должность;
- направление службы занятости;
- характеристики;
- рекомендательные письма;

- справки, подтверждающие период работы у работодателя и размер заработной платы;
- наградные документы;
- листки нетрудоспособности;
- медицинские справки;
- справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям;
- иные документы, содержащие персональные сведения о работнике.

6.9. Документами, содержащими персональные данные воспитанников, их родителей (законных представителей) и иных лиц, являются:
- документы, удостоверяющие личность (паспорт, свидетельство о рождении);
- документы о регистрации по месту жительства;
- полис медицинского страхования;
- документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний, медицинское заключение об отсутствии противопоказаний для пребывания в дошкольной образовательной организации и т.п.);
- документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.);
- иные документы, содержащие персональные данные (в том числе сведения, необходимые для предоставления воспитаннику гарантий и компенсаций, установленных действующим законодательством).

6.10. Комплекс документов, сопровождающий процесс оформления трудовых отношений работника в Организации при его приеме, переводе и увольнении.

6.10.1. Информация, представляемая работником при поступлении на работу в Организацию, должна иметь документальную форму. При заключении трудового договора в соответствии со статьей 65 Трудового кодекса Российской Федерации лицо, поступающее на работу, предъявляет работодателю:
- паспорт или иной документ, удостоверяющий личность;
- трудовую книжку, за исключением случаев, когда трудовой договор заключается впервые или работник поступает на работу на условиях совместительства, либо трудовая книжка у работника отсутствует в связи с ее утратой или по другим причинам;
- страховое свидетельство государственного пенсионного страхования;
- документы воинского учета - для военнообязанных и лиц, подлежащих воинскому учету;
- документ об образовании, о квалификации или наличии специальных знаний - при поступлении на работу, требующую специальных знаний или специальной подготовки;
- свидетельство о присвоении ИНН (при его наличии у работника).

6.10.2. При оформлении работника в Организацию специалистом по кадрам заполняется унифицированная форма Т-2 «Личная карточка работника», в которой отражаются следующие анкетные и биографические данные работника:
- общие сведения (Ф.И.О. работника, дата рождения, место рождения, гражданство, образование, профессия, стаж работы, состояние в браке, паспортные данные);
- сведения о воинском учете;
- данные о приеме на работу;

В дальнейшем в личную карточку вносятся:
- сведения о переводах на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;

- сведения о профессиональной переподготовке;
- сведения о наградах (поощрениях), почетных званиях;
- сведения об отпусках;
- сведения о социальных гарантиях;
- сведения о месте жительства и контактных телефонах.

6.10.3. Специалистом по кадрам Организации создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

6.10.3.1.Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Организации, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

6.10.3.2.Документация по организации работы (должностные инструкции работников, приказы, распоряжения, указания руководства Организации); документы по планированию, учету, анализу и отчетности в части работы с персоналом Организации.

6.11. В зависимости от состава персональных данных определяется категория, к которой они относятся:

- категория 1: персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
- категория 2: персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3: персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4: обезличенные и (или) общедоступные персональные данные.

7. Сроки обработки персональных данных

7.1.Сроки обработки персональных данных определяются в соответствии со сроком действия договора с субъектом персональных данных, Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», а также иными требованиями законодательства РФ и нормативными документами.

7.2.В Организации создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в Организации данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

8. Порядок и условия обработки, хранения и использования персональных данных

8.1.Документы, содержащие персональные данные, создаются путём:

а) копирования оригиналов;

б) внесения сведений в учётные формы (на бумажных и электронных носителях);

в) получения оригиналов необходимых документов.

8.2. Порядок получения персональных данных.

8.2.1. Все персональные данные субъекта получаются Организацией у него самого или у его законного представителя, за исключением случаев, если их получение возможно только у третьей стороны.

Должностное лицо работодателя должно сообщить работнику Организации о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

При отказе субъекта (его законного представителя) от дачи согласия на получение персональных данных у иного лица составляется акт, который подписывается не менее чем тремя лицами, из числа работников Организации.

8.2.2. Организация не имеет права получать и обрабатывать персональные данные субъекта о его политических, религиозных и иных убеждениях и частной жизни, в том числе персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством. В случаях, непосредственно связанных с вопросами трудовых отношений, образовательной деятельности, в соответствии со статьёй 24 Конституции Российской Федерации, Организация вправе получать и обрабатывать данные о частной жизни субъекта только с его письменного согласия (согласия его законного представителя).

8.3. Обработка Оператором указанных персональных данных работников Организации возможна только с их согласия либо без их согласия в следующих случаях:

- персональные данные являются общедоступными;
- персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;
- по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

8.4. Оператор вправе обрабатывать персональные данные работников Организации только с их письменного согласия.

8.4.1. Письменное согласие работника на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- наименование (фамилию, имя, отчество) и адрес Оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Оператором способов обработки персональных данных;
- срок, в течение которого действует согласие, а также порядок его отзыва.

8.4.2. Форма заявления о согласии работника на обработку персональных данных является приложением настоящей Политике (приложение № 1 к настоящей Политике).

8.5. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных (его законным представителем).

В случае отзыва субъектом персональных данных (его законным представителем) согласия на обработку персональных данных Организация вправе продолжить обработку персональных данных без согласия субъекта персональных данных (его законного представителя) при наличии оснований, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

8.6. Согласие работника Организации не требуется в следующих случаях, если:

- обработка персональных данных осуществляется на основании Трудового кодекса РФ или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия Оператора;
- обработка персональных данных осуществляется в целях исполнения трудового договора;
- обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;
- обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно

8.7. Порядок обработки персональных данных.

8.7.1. Работник Организации предоставляет Оператору (ответственному должностному лицу, специалисту по кадрам) достоверные сведения о себе. Ответственный работник проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

8.7.2. В соответствии со статьёй 86 главы 14 Трудового кодекса Российской Федерации в целях обеспечения прав и свобод человека и гражданина Оператор при обработке персональных данных работника Организации должен соблюдать следующие общие требования:

- обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания, обрабатываемых персональных данных Оператор должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;
- при принятии решений, затрагивающих интересы работника, Оператор не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения;
- защита персональных данных работника от неправомерного их использования или утраты обеспечивается Оператором за счет его средств в порядке, установленном федеральным законом;
- работники и их представители должны быть ознакомлены под расписку с документами Организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области;
- во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

8.8. Порядок передачи персональных данных.

При передаче персональных данных работника Оператор должен соблюдать следующие требования:

8.8.1. Не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом.

8.8.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия.

8.8.3. Предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

8.8.4. Осуществлять передачу персональных данных работников в пределах Организации в соответствии с настоящей Политикой.

8.8.5. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции.

8.8.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

8.8.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

8.9. Порядок хранения персональных данных.

8.9.1. Хранение и обработка персональных данных может осуществляться с использованием электронных систем, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих обрабатывать такие данные с использованием средств автоматизации. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в информационной системе информационные технологии. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующей информации на основании приказа руководителя Организации.

8.9.2. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде, компьютерной программе «1С: Предприятие», ПО УТЗП «АМБа».

8.9.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены Оператору на основании федерального закона или если персональные данные являются общедоступными)

Оператор до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес Оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные настоящим Федеральным законом права субъекта персональных данных.

8.10. Персональные данные субъектов хранятся на бумажных и электронных носителях в специально предназначенных для этого помещениях, в местах, обеспечивающих защиту от несанкционированного доступа. Защита персональных данных включает в себя установление особого режима доступа в те помещения, где хранятся такие данные, направленного на защиту от несанкционированного доступа к ним, изменений или распространения.

8.11. В процессе хранения персональных данных субъектов должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;
- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством Российской Федерации и настоящей Политикой;
- контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

8.12. Перечень должностных лиц, имеющих право доступа к персональным данным, состав персональных данных, к которым имеют доступ должностные лица Организации, места хранения документов, содержащих персональные данные, устанавливаются приказом руководителя Организации.

8.13. Лица, имеющие доступ к персональным данным обязаны использовать персональные данные лишь в целях, для которых они были предоставлены.

8.14. Персональные данные работника используются для целей, связанных с выполнением трудовых функций, в том числе для решения вопросов аттестации, формирования учебного плана, составления отчетов в вышестоящие организации, формирования различных баз данных, продвижения работников по службе, установления размера зарплаты.

8.15. Персональные данные воспитанников, их родителей (законных представителей) используются для целей, связанных с осуществлением образовательного процесса, в том числе для формирования групп, составления учебного плана, составления отчетов в вышестоящие организации, формирования различных баз данных, для возможности поддерживать связь с родителями (законными представителями), учитывать особенности воспитанника при его обучении и воспитании.

9. Передача персональных данных

9.1. При передаче персональных данных работников, воспитанников (их родителей (законных представителей)) другим юридическим и физическим лицам Организация должна соблюдать следующие требования:

- персональные данные не могут быть сообщены третьей стороне без письменного согласия работника, родителей (законных представителей) воспитанника, за исключением случаев, когда это необходимо для предупреждения угрозы жизни и здоровью работника, воспитанника, а также в случаях, установленных федеральным законом;
- лица, получающие персональные данные работника, воспитанника (его родителей (законных представителей)) предупреждаются о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное

положение не распространяется на обмен персональными данными в порядке, установленном федеральными законами.

9.2. Передача персональных данных субъекта представителям может быть осуществлена в установленном действующим законодательством порядке только в том объеме, который необходим для выполнения указанными представителями их функций.

10. Доступ к персональным данным работников

10.1. Право доступа к персональным данным работников Организации имеют:

- руководитель 1 уровня Организации (заведующий);
- руководители 2 уровня Организации (заместитель заведующего по воспитательной и методической работе, заместитель заведующего по административно – хозяйственной части);
- работники бухгалтерии (главный бухгалтер, бухгалтер);
- специалист по кадрам;
- специалист по охране труда;
- делопроизводитель (информация о фактическом месте проживания и контактные телефоны работников);

10.2. Работник Организации имеет право:

10.2.1. получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные работника;

10.2.2. требовать от Оператора уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющих необходимыми для Организации персональных данных;

10.2.3. получать от Оператора:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;
- сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

10.2.4. требовать извещения Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях; обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Оператора при обработке и защите его персональных данных.

10.3. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения руководителя Организации.

10.4. Передача информации третьей стороне возможна только при письменном согласии работников Организации.

11. Порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований

11.1. Уничтожение документов, содержащих персональные данные, производится:

- по достижении целей их обработки согласно номенклатуре дел и документов;
- по достижении окончания срока хранения персональных данных, оговоренного в соответствующем соглашении заинтересованных сторон; в том числе, если они не подлежат архивному хранению.

11.2. Уничтожение документов, содержащих персональные данные, производится в случае выявления неправомерной обработки персональных данных в срок, не превышающий десяти рабочих дней с момента выявления неправомерной обработки персональных данных.
11.3. Уничтожение информации с персональными данными, хранящейся в электронном виде на материальных носителях, производиться путем выполнения процедуры специальной подготовки материальных носителей (многократное форматирование разделов, выделенных под хранение данных).
11.4. Уничтожение материальных носителей с персональными данными осуществляется механическим либо электромагнитным воздействием с помощью специализированных средств (шредер, уничтожитель оптических дисков и т.п.). Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.
11.5. Уничтожение производится по мере необходимости, в зависимости от объёмов, накопленных для уничтожения документов.
11.6. Для уничтожения материальных носителей и информации на материальных носителях документально создается экспертная комиссия в составе не менее 2 человек. Уничтожение осуществляется по акту. Уничтожение документов производится в присутствии всех членов комиссии, которые несут персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (состав комиссии утверждается приказом руководителя дошкольной образовательной организации). После уничтожения материальных носителей членами комиссии подписывается акт в трех экземплярах (приложение № 2 к настоящей Политике) делается запись в журналах их учёта и регистрации (приложение № 3 к настоящей Политике), а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».
11.7. Накапливаемые для уничтожения документы, копии документов, черновики, содержащие персональные данные, должны храниться отдельно.

12. Права Оператора и субъектов персональных данных на обеспечение защиты персональных данных

12.1. Организация как Оператор персональных данных, вправе:
- 12.1.1. отстаивать свои интересы в суде;
- 12.1.2. предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- 12.1.3. отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;
- 12.1.4. использовать персональные данные субъекта без его согласия, в случаях, предусмотренных законодательством.

12.2. Субъект персональных данных имеет право:
- 12.2.1. требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- 12.2.2. требовать перечень своих персональных данных, обрабатываемых Оператором и источник их получения;
- 12.2.3. получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;

12.2.4. требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;

12.2.5. обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;

12.2.6. на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

13. Обязанности субъекта персональных данных по обеспечению по обеспечению достоверности его персональных данных

13.1. В целях обеспечения достоверности персональных данных работники обязаны:

13.1.1. При приеме на работу в Организацию представлять уполномоченным работникам достоверные сведения о себе в порядке и объеме, предусмотренном законодательством Российской Федерации.

13.1.2. В случае изменения персональных данных работника: фамилия, имя, отчество, адрес места жительства, паспортные данные, сведения об образовании, состоянии здоровья (вследствие выявления в соответствии с медицинским заключением противопоказаний для выполнения работником его должностных, трудовых обязанностей и т.п.) сообщать об этом в течение 5 рабочих дней от даты их изменений.

13.2. В целях обеспечения достоверности персональных данных воспитанников:

13.2.1. Родители (законные представители) воспитанников при приеме в Организацию предоставляют уполномоченным его работникам достоверные сведения о себе и своих несовершеннолетних детях.

13.2.2. В случае изменения сведений, составляющих персональные данные воспитанника, родители (законные представители) несовершеннолетнего обязаны в течение месяца сообщить об этом уполномоченному работнику Организации.

14. Ответственность за нарушение Политики

14.1. За нарушение настоящей Политики обработки (сбора, хранения, использования, распространения и защиты) персональных данных должностные лица несут ответственность в соответствии с действующим законодательством.

14.2. За нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю, работник несет материальную ответственность в соответствии с действующим трудовым законодательством.

14.3. Материальный ущерб, нанесенный субъекту персональных данных за счет ненадлежащего хранения и использования персональных данных, подлежит возмещению в порядке, установленном действующим законодательством.

14.4. Организация вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с Оператором трудовые отношения (работникам);
- полученных Оператором в связи с заключением договора, стороной которого является субъект персональных данных (воспитанник и др.), если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются Организацией исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- являющихся общедоступными персональными данными;

- включающих в себя только фамилии, имена и отчества субъектов персональных данных;
- необходимых в целях однократного пропуска субъекта персональных данных на территорию Организации или в иных аналогичных целях;
- включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;
- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Во всех остальных случаях Организация (руководитель и (или) уполномоченные им лица) обязаны направить в уполномоченный орган по защите прав субъектов персональных данных соответствующее уведомление.

15. Реализуемые требования к защите информации, составляющей персональные данные

15.1. Организация предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

15.2. Защита информации в информационной системе персональных данных является неотъемлемой составной частью деятельности Организации и должна осуществляться во взаимосвязи с другими мерами по защите информации, составляющей персональные данные.

15.3. Защита информации является составной частью работ по созданию и эксплуатации информационной системы персональных данных и должна осуществляться в установленном Политикой порядке и реализовываться в виде системы (подсистемы) защиты персональных данных.

15.4. Защита информации должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счет несанкционированного доступа к ней, по предупреждению преднамеренных программно - технических воздействий с целью нарушения целостности (уничтожения, искажения) информации в процессе ее обработки, передачи и хранения, нарушения ее санкционированной доступности и работоспособности технических средств.

15.5. В информационной системе персональных данных должны использоваться сертифицированные по требованиям безопасности информации средства защиты информации и (или) технические и организационные решения, исключающие утечку информации по техническим каналам, за счет несанкционированного доступа, предупреждающие нарушение целостности информации и ее санкционированной доступности.

15.6. Защита информации должна быть дифференцированной в зависимости от применяемых технических средств, обрабатывающих информацию, составляющую персональные данные, установленного уровня защищенности информационной системы персональных данных, установленного класса и утвержденной для нее модели угроз.

15.7. Все используемые в информационной системе персональных данных средства защиты информации должны быть проверены на соответствие ограничениям и условиям эксплуатации, изложенным в сертификате соответствия, эксплуатационной

документации или формуляре (для технических и программных средств защиты информации соответственно).

15.8. Обработка информации, составляющей персональные данные осуществляется на основании письменного разрешения (приказа) руководителя Организации.

15.9. В целях координации действий по обеспечению безопасности персональных данных в Организации назначается ответственное лицо за обеспечение безопасности персональных данных.

16. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

16.1. Работники Организации, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

16.2. Руководитель Организации за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, несет административную ответственность согласно статьи 5.27 и статьи 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные работника.

Приложение № 1 к Политике

Заведующему МБДОУ
«ДСОВ «Аленький цветочек»
С.Н. Куделькиной

от _____

_____
(фамилия, имя, отчество)
паспорт (серия, номер)
выдан
_____
_____
_____
зарегистрированной(ого) по адресу:
_____
_____

ЗАЯВЛЕНИЕ
О СОГЛАСИИ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Настоящим я, _____,
представляю МБДОУ «ДСОВ «Аленький цветочек» (далее по тексту - Оператор)

ОГРН 1038600200033, ИНН 8614005936, зарегистрированному по адресу: Россия, Тюменская область, Ханты-Мансийский автономный округ - Югра, Октябрьский район, село Перегрёбное, ул. Лесная, д. 36, почтовый индекс 628109, свои персональные данные в целях обеспечения соблюдения трудового законодательства и иных нормативно-правовых актов при содействии в трудоустройстве, обучении и продвижении по работе, обеспечения личной моей безопасности, текущей трудовой деятельности, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Моими персональными данными является любая информация, относящаяся ко мне как к физическому лицу (субъекту персональных данных), указанная в трудовом договоре, личной карточке работника (унифицированная форма Т-2), трудовой книжке и полученная в течение срока действия настоящего трудового договора, в том числе: мои фамилия, имя, отчество, год, месяц, дата и место рождения, гражданство, документы, удостоверяющие личность, идентификационный номер налогоплательщика, номер страхового свидетельства государственного пенсионного страхования, адреса фактического места проживания и регистрации по месту жительству, почтовые и электронные адреса, номера телефонов, фотографии, сведения об образовании, профессии, специальности и квалификации, семейном положении и составе семьи, сведения об имущественном положении, доходах, задолженности, занимаемых ранее должностях и стаже работы, воинской обязанности; наличие загранпаспорта, наличие и категорию водительских прав, наличие судимости, данные об опыте работы; сведения о трудовом договоре и его исполнении (занимаемые должности, существенные условия труда, сведения об аттестации, повышении квалификации и профессиональной переподготовке, поощрениях и наказаниях, видах и периодах отпуска, временной нетрудоспособности, социальных льготах, командировании, рабочем времени и пр.), а также о других договорах (индивидуальной, коллективной материальной ответственности, ученических, оказания услуг и т. п.), заключаемых при исполнении трудового договора.

Своей волей и в своих интересах выражаю согласие на осуществление Оператором любых действий в отношении моих персональных данных, которые необходимы или

желаемы для достижения указанных целей, в том числе выражаю согласие на обработку без ограничения моих персональных данных, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т. ч. передачу), обезличивание, блокирование, уничтожение персональных данных при автоматизированной и без использования средств автоматизации обработке; запись на электронные носители и их хранение; передачу Оператором по своему усмотрению данных и соответствующих документов, содержащих персональные данные, третьим лицам, включая банки, налоговые органы, в отделения пенсионного фонда, фонда социального страхования, фонда обязательного медицинского страхования, уполномоченным агентам и организациям; хранение моих персональных данных в течение 75 лет, содержащихся в документах, образующихся в деятельности Оператора, согласно части 1 статьи 17 Закона от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», а также при осуществлении любых иных действий с моими персональными данными, указанными в трудовом договоре и полученными в течение срока действия трудового договора, в соответствии с требованиями действующего законодательства РФ и Закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Настоящее согласие на обработку персональных данных действует с момента представления бессрочно и может быть отозвано мной при представлении Оператору заявления в простой письменной форме в соответствии с требованиями законодательства Российской Федерации.

Обязуюсь сообщать в течение 5 (пяти) рабочих дней об изменении места жительства, контактных телефонов, паспортных, документных и иных персональных данных. Об ответственности за достоверность представленных персональных сведений предупрежден(а).

Подтверждаю, что с Политикой Оператора в отношении обработки и защиты персональных данных ознакомлен(а).

_____	_____	_____
(дата)	(личная подпись)	(расшифровка: инициалы, фамилия)

Приложение № 2 к Политике

Акт
№ _____ от _____ (дата)
об уничтожении носителей, содержащих персональные данные

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор бумажных, электронных, магнитных и оптических носителей персональных данных и другой конфиденциальной информации (далее носители) и установила, что в соответствии с требованиями руководящих документов по защите информации указанные носители и информация, записанная на них в процессе эксплуатации, в соответствии с действующим законодательством Российской Федерации, подлежит гарантированному уничтожению и составила настоящий акт о том, что произведено уничтожение носителей персональных данных в составе:

№ п/п	Дата	Тип носителя	Учетный номер носителя	Категория информации	Примечание

Всего носителей _____
(цифрами и прописью количество)

На указанных носителях персональные данные уничтожены путем
_____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители персональных данных уничтожены путем
_____.
(разрезания/сжигания/размагничивания/физического уничтожения/механического уничтожения / иного способа)

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

Приложение № 3 к Политике

ЖУРНАЛ
уничтожения носителей персональных данных
в Муниципальном бюджетном дошкольном образовательном учреждении
«Детский сад общеразвивающего вида «Аленький цветочек»

Журнал начат ____ _____
Журнал завершен ____ _____
Ответственный _____ (Ф.И.О.)
На _____ листах

№ п/п	Наименование Информационной системы персональных данных, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные сданные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных
1	2	3	4	5	6	7	8

Приложение № 2
к приказу от 16.08.2017 № 533 - од

ПРАВИЛА
осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к защите персональных данных
в Муниципальном бюджетном дошкольном образовательном учреждении
«Детский сад общеразвивающего вида «Аленький цветочек»
(далее по тексту - Правила)

1. Общие положения

1.1. Настоящие Правила в Муниципальном бюджетном дошкольном образовательном учреждении «Детский сад общеразвивающего вида «Аленький цветочек» (далее – ДОО или дошкольная образовательная организация), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона РФ от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «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», утвержденных постановлением Правительства РФ от 21.03.2012 № 211.

1.3. Для обработки ПДн, необходимых для предоставления государственных и муниципальных услуг в ДОО используется информационная система персональных данных (далее – ИСПДн) «ИАС «Аверс: Управление дошкольной образовательной организацией», предназначенная для осуществления деятельности дошкольной образовательной организации, согласно Устава.

1.4. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в ДОО, в соответствии с Трудовым кодексом Российской Федерации, используется ИСПДн «ИАС «Аверс: Управление дошкольной образовательной организацией» и ИСПДн «АМБА».

1.5. Пользователем ИСПДн (далее – Пользователь) является сотрудник дошкольной образовательной организации, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее – СЗИ) ИСПДн.

1.6. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн дошкольной образовательной организации проводятся в следующих целях:

1.6.1. проверка выполнения требований организационно-распорядительной документации по защите информации в дошкольной образовательной организации и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.6.2. оценка уровня осведомленности и знаний работников ДОО в области обработки и защиты персональных данных;
1.6.3. оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в ДОО разделяются на следующие виды:

— регулярные;
— плановые;
— внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АИС периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в ДОО.

2.3.Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн дошкольной образовательной организации.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 по решению руководителя дошкольной образовательной организации.

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в Отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчет передается на рассмотрение руководителю ДОО.

4.4. Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в ДОО (приложение 2).

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных ДОО.

5.2. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех ответственных и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполнятся следующие проверки:

- Соответствие полномочий Пользователя правилам доступа.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в ДОО.
- Соблюдение Порядка доступа в помещения ДОО, где ведется обработка персональных данных.
- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении внештатных ситуаций.
- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в ДОО.
- Порядок и условия применения средств защиты информации.
- Состояние учета машинных носителей персональных данных.
- Наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер.
- Проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.
- Технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.
- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

Приложение № 1 к Правилам

ПЛАН
внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС ДОО СПО	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обеспечения резервного копирования		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Организация анализа и		Ежегодно	Ответственный за

пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз			обеспечение безопасности персональных данных информационных систем персональных данных
Поддержание в актуальном состоянии нормативно-организационных документов		Ежемесячно	Ответственный за организацию обработки ПДн в ДОО
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	

Приложение № 2 к Правилам

ПРОТОКОЛ № ____
проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных в МБДОУ «ДСОВ «Аленький цветочек»

Настоящий Протокол составлен в том, что «__»_____201_ г.
_____ (комиссией)
(должность, Ф.И.О. сотрудника)
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:
фамилия и инициалы / подпись / должность

Члены комиссии:
фамилия и инициалы / подпись / должность
фамилия и инициалы / подпись / должность

Приложение № 3
к приказу от 16.08.2017 № 533 - од

ПОРЯДОК
обращения с информацией, подлежащей защите
(далее по тексту - Порядок)

1. Общие положения

1.1. Настоящий Порядок разработан с целью соблюдения надлежащих правил обращения с не содержащими государственной тайны конфиденциальными и другими защищаемыми сведениями, а также защиты прав и интересов Муниципального бюджетного дошкольного образовательного учреждения «Детский сад общеразвивающего вида «Аленький цветочек» (далее по тексту – дошкольная образовательная организация или ДОО), его клиентов и корреспондентов в случае неправомерного обращения с защищаемой информацией.

1.2. Дошкольная образовательная организация, как собственник (владелец) информации, принимает меры по защите банковской тайны, персональных данных, служебной тайны, своей коммерческой тайны и другой информации в соответствии с предоставленными ему действующим законодательством правами и обязанностями.

1.3. К категориям конфиденциальных относятся сведения, удовлетворяющие следующим критериям:
- — они не являются общеизвестными или общедоступными на законных основаниях;
- — монопольное обладание этими сведениями даёт ДОО коммерческие преимущества, экономическую и иную выгоду и разглашение или открытое использование которых может привести к нанесению ущерба (материального, морального, физического) дошкольной образовательной организации, его клиентам или корреспондентам (коммерческая тайна);
- — в отношении которых дошкольная образовательная организация обязана обеспечить реализацию необходимых мер защиты (банковская тайна, персональные данные, служебная тайна);
- — эти сведения не защищены действующим законодательством (авторским, патентным правом и т.п.).

1.4. Под банковской тайной понимаются сведения об операциях, счетах и вкладах, а также сведения о клиентах и корреспондентах Банка, подлежащие обязательной защите согласно статье 26 Закона РФ «О банках и банковских деятельности» и статье 857 Гражданского кодекса РФ.

1.5. Под служебной тайной понимаются сведения, не являющиеся банковской тайной, и подлежащие обязательной защите согласно Перечня сведений ограниченного распространения в ДОО.

1.6. Под коммерческой тайной ДОО понимаются сведения, связанные с производством, технологией, управлением, финансами и другой деятельностью дошкольной образовательной организации, разглашение (передача, утечка, открытое использование) которых может привести к нанесению ущерба ДОО, участникам образовательных отношений.

1.7. Под персональными данными понимаются сведения о фактах, событиях и обстоятельствах частной жизни граждан, позволяющие идентифицировать их личность.

1.8. Перечень сведений (информационных ресурсов), составляющих банковскую тайну определяется в соответствии с Законом РФ «О банках и банковских деятельности».

1.9. Перечень сведений (информационных ресурсов), составляющих коммерческую тайну ДОО, неправильное обращение с которыми может нанести ущерб их собственнику, владельцу или иному лицу, определяется руководителем ДОО на основании предоставленных действующим законодательством прав.

1.10. Указанные перечни оформляются в виде «Перечня информационных ресурсов, подлежащих защите».

Кроме конфиденциальной информации в данный «Перечень информационных ресурсов, подлежащих защите» включается информация, подлежащая защите в силу того, что нарушение ее целостности (искажение, фальсификация) или доступности (уничтожение, блокирование) может привести к нанесению ощутимого ущерба ДОО, участникам образовательных отношений.

1.11. ДОО, как собственник (владелец) информации, составляющей коммерческую тайну, имеет право передавать её другим юридическим и физическим лицам при условии, что данная сделка не противоречит обязательствам дошкольной образовательной организации, не ущемляет права и не наносит вред самой ДОО, участникам образовательных отношений.

Раскрытие юридическим или физическим лицам коммерческой тайны ДОО возможно в случае привлечения их к совместной хозяйственной, финансовой и иной деятельности, требующей передачи конфиденциальных сведений, и только в том объеме, который необходим для реализации целей и задач ДОО, а также при условии принятия ими на себя обязательств по неразглашению и исключению неправомерного использования полученных сведений.

Право принятия решения на передачу (предоставление) конфиденциальных сведений третьим лицам предоставлено только руководителю дошкольной образовательной организации.

Конфиденциальные сведения других юридических или физических лиц, переданные ДОО для выполнения работ или осуществления иной совместной деятельности, и в отношении которых ДОО взяла на себя обязательство о неразглашении и исключении неправомерного их использования, подлежат защите наравне с другими сведениями, составляющими коммерческую тайну ДОО.

Вся информация, предоставляемая раскрывающей стороной получающей стороне, остается исключительной собственностью раскрывающей стороны.

Информация не считается коммерческой тайной, а получающая ее сторона не будет иметь никаких обязательств в отношении данной информации, если она:

- стала известна получающей стороне в результате неправильного обращения или хранения раскрывающей стороной;
- стала известна получающей стороне от третьих лиц;
- независимо разработана получающей стороной, при условии, что лицо или лица, разработавшие ее, не имели доступа к конфиденциальной информации раскрывающей стороны.

Передача сведений, составляющих банковскую тайну, осуществляется в строгом соответствии с действующим законодательством.

1.12. Каждый сотрудник ДОО обязан сохранять банковскую, служебную и коммерческую тайну и соблюдать требования обращения с защищаемой информацией, ставшей ему известной (или доступной для манипулирования) в процессе работы. Свои обязательства по сохранению коммерческой тайны дошкольной образовательной организации он подтверждает при заключении трудового договора, подписывая «Соглашение (обязательство) о соблюдении требований обращения с защищаемой информацией» (Приложение 1 к настоящему Порядку).

Каждый сотрудник обязан знать и выполнять требования настоящего документа и принимать меры по предотвращению несанкционированной утечки (разглашения), искажения, блокирования или уничтожения используемой им в работе информации, подлежащей защите в соответствии с «Перечнем информационных ресурсов, подлежащих защите».

В случае отсутствия, по мнению исполнителя, в Перечне информационных ресурсов, подлежащих защите» тех или иных подлежащих защите сведений, он обязан в

кратчайший срок представить в комиссию по технической защите информации ДОО свои предложения о внесении в «Перечень информационных ресурсов, подлежащих защите» необходимых дополнений (изменений) и принятия мер по защите соответствующих информационных ресурсов.

1.13. Ответственными за принятие необходимых организационных и технических мер безопасности и соблюдение сотрудниками ДОО требований обращения с защищаемой информацией являются члены комиссии по защите информации ДОО.

2. Порядок учета, хранения и уничтожения документов и магнитных носителей информации

2.1. В ДОО учёт документов и магнитных носителей с защищаемой информацией осуществляется лицами (далее - делопроизводителями), которым поручен прием и учет несекретной документации.

2.2. На документах, содержащих сведения ограниченного распространения, проставляется пометка «Для служебного пользования» (сокращённо «ДСП»).

Указанная пометка и номер экземпляра проставляются в правом верхнем углу первой страницы документа. Использовать другие ограничительные пометки или грифы («Конфиденциально», «Банковская тайна» и т.п.) запрещается.

Отнесение конкретных документов к документам «ДСП» производится исполнителем (разработчиком) и(или) лицом, подписывающим (утверждающим) документ на основании «Перечня информационных ресурсов, подлежащих защите».

2.3. Документы с пометкой «Для служебного пользования»:

- учитываются, как правило, отдельно от несекретной информации. При незначительном объеме таких документов разрешается вести их учет совместно с другими несекретными документами. К регистрационному номеру (индексу) документа добавляется отметка «ДСП»;
- на последнем листе (на оборотной стороне) должно быть указано количество экземпляров, фамилия исполнителя, номер его телефона и дата печати. Отпечатанные и подписанные документы вместе с черновиками и вариантами передаются для делопроизводства. Черновики и варианты уничтожаются делопроизводителем с отражением факта уничтожения в учетных формах. Недописанные по каким-либо причинам проекты документов уничтожаются лично исполнителем;
- после регистрации передаются сотрудникам под расписку;
- пересылаются сторонним организациям заказными почтовыми отправлениями, а при наличии соответствующего договора через органы спецсвязи;
- размножаются (тиражируются) с разрешения руководителя ДОО. Разрешение оформляется на последнем листе (на оборотной стороне) размножаемого документа. Учет размноженных документов осуществляется поэкземплярно;
- хранятся в надежно запираемых и опечатываемых шкафах (ящиках, хранилищах).

2.3.1. Требования пунктов настоящего Порядка распространяется и на съемные машинные носители информации, содержащие сведения ограниченного распространения. Используемые для записи защищаемой информации носители должны быть учтены у делопроизводителей ДОО. На магнитном носителе проставляются регистрационный номер, пометка «Для служебного пользования», дата и роспись работника, отвечающего за учет носителей.

2.3.2. При необходимости направления документов с пометкой «Для служебного пользования» в несколько адресов составляется указатель рассылки, в котором поадресно проставляются номера экземпляров отправляемых документов. Указатель рассылки подписывается исполнителем и руководителем подразделения, готовившего документ.

2.3.3. Исполненные документы с пометкой «Для служебного пользования» группируются в дела в соответствии с номенклатурой дел несекретного делопроизводства. На обложке

дела, в которое помещены такие документы, также проставляется пометка «Для служебного пользования».

2.3.4. Уничтожение дел, документов, машинных носителей с пометкой «Для служебного пользования», утративших свое практическое значение и не имеющих исторической ценности, производится по акту. В учетных формах об этом делается отметка со ссылкой на соответствующий акт.

2.3.5. Передача документов и дел с пометкой «Для служебного пользования» от одного работника другому осуществляется с разрешения руководителя ДОО, с отметкой в соответствующих журналах учета.

2.3.6. При смене работника, ответственного за учет документов с пометкой «Для служебного пользования», составляется акт приема-сдачи этих документов, который утверждается руководителем ДОО.

2.3.7. Проверка наличия документов, магнитных носителей информации и дел с пометкой «Для служебного пользования» проводится один раз в год комиссией, назначаемой приказом руководителя ДОО. Результаты проверки оформляются актом. Проверка наличия документов и порядка обращения с ними при необходимости может проводиться соответствующими членами комиссии по защите информации, а также лицом, которому поручен прием и учет документации ограниченного распространения.

3. Ответственность за нарушение правил обращения с защищаемой информацией

3.1. В случае невыполнения требований настоящего документа и нанесения ДОО, участникам образовательных отношений материального или иного ущерба, к получающей стороне (сотруднику, организации) предъявляются требования о его возмещении в соответствии с действующим законодательством.

3.2. За разглашение (несанкционированную передачу третьим лицам и т.п.) сведений, содержащих персональные данные или составляющих коммерческую тайну должностные лица (сотрудники) ДОО несут уголовную (ст. 183 УК РФ), гражданскую (ст. 139, 857 ГК РФ) или дисциплинарную ответственность в порядке, определяемом действующим законодательством и внутренними нормативными актами ДОО.

3.3. Получающая сторона несет ответственность за:

— разглашение конфиденциальных сведений (составляющих, коммерческую тайну или персональных данных) вследствие их неправильного хранения или использования;

— не пресечение разглашения или неправомерного использования конфиденциальных сведений, после обнаружения факта разглашения.

3.4. За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ (автоматизированной системы обработки информации), уничтожение, блокирование или модификация защищаемой ДОО информации, сотрудники дошкольной образовательной организации несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

Приложение № 1 к Порядку

СОГЛАШЕНИЕ (ОБЯЗАТЕЛЬСТВО)
о соблюдении требований обращения с защищаемой информацией

«___»_____2017 г.

Муниципальное бюджетное дошкольное образовательное учреждение «Детский сад общеразвивающего вида «Аленький цветочек», именуемое в дальнейшем ДОО, в лице руководителя ДОО Куделькиной Светланы Николаевны, с одной стороны,

и _____,

именуемый (ая) в дальнейшем ДЕЛОПРОИЗВОДИТЕЛЬ, с другой стороны, заключили настоящее соглашение о том, что:

1. ДЕЛОПРОИЗВОДИТЕЛЮ будет предоставлен доступ к конфиденциальным и другим защищаемым ДОО сведениям, необходимым ей для выполнения своих функциональных обязанностей (согласно занимаемой должности).
2. ДЕЛОПРОИЗВОДИТЕЛЬ обязуется:
   - хранить тайну по операциям, счетам и вкладам ДОО, участников образовательных отношений (банковскую тайну);
   - во время работы в ДОО и в течение 3-х лет после увольнения не раскрывать (не передавать) третьим лицам ставшие ему известными конфиденциальные (защищаемые ДОО) сведения (за исключением случаев привлечения последних к деятельности, требующей раскрытия такой информации и только в объеме, необходимом для реализации целей и задач ДОО, с письменного разрешения руководителя ДОО);
   - не использовать ставшие ему известными или разработанные им конфиденциальные сведения иначе, как в интересах ДОО;
   - соблюдать указанные в «Порядке обращения с информацией, подлежащей защите» требования и правила обеспечения информационной безопасности ДОО;
   - в случае прекращения работы в ДОО, сразу же возвратить ДОО все документы и другие материалы, содержание которых отнесено к конфиденциальной и иной защищаемой ДОО информации, полученные в ходе выполнения ДЕЛОПРОИЗВОДИТЕЛЕМ своих служебных обязанностей.
3. ДЕЛОПРОИЗВОДИТЕЛЬ подтверждает, что:
   - он(она) ознакомлен(а) с требованиями «Порядка обращения с информацией, подлежащей защите»;
   - он(она) не имеет перед кем-либо никаких обязательств, которые входят в противоречие с настоящим соглашением или ограничивают его(ее) деятельность в ДОО.

_____ (подпись, ФИО ДЕЛОПРОИЗВОДИТЕЛЯ)

Приложение № 4
к приказу от 16.08.2017 № 533 – од

ПОРЯДОК
резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации (СЗИ)

1. Назначение и область действия

1.1. Порядок резервирования и восстановления работоспособности технических средств (ТС) и программного обеспечения (ПО), баз данных и средств защиты информации (СЗИ) (далее – Инструкция), связанные с функционированием ИСПДн в Муниципальном бюджетном дошкольном образовательном учреждении «Детский сад общеразвивающего вида «Аленький цветочек» (далее по тексту ДОО или дошкольная образовательная организация), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.2. Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

1.3. Задачей данной Инструкции является:
- определение мер защиты от потери информации;
- определение действий восстановления в случае потери информации.

1.4. Действие настоящей Инструкции распространяется на всех пользователей ДОО, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.5. Пересмотр настоящей Инструкции осуществляется по мере необходимости, но не реже одного раза в два года.

1.6. Ответственным сотрудником за реагирование на инциденты безопасности, приводящие к потере защищаемой информации, назначается Администратор ИСПДн.

1.7. Ответственным сотрудником за контроль обеспечения мероприятий по предотвращению инцидентов безопасности, приводящих к потере защищаемой информации, назначается Администратор безопасности.

2. Порядок реагирования на инцидент

2.1. В настоящей Инструкции под Инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:
- в результате непреднамеренных действий пользователей;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

2.3. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники ДОО, Администратор и Оператор ИСПДн, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. Технические меры

3.1.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

3.1.2. Системы жизнеобеспечения ИСПДн включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.1.3. Все критичные помещения ДОО (помещения, в которых размещаются элементы ИСПДн и средства защиты) оборудуются средствами пожарной сигнализации и пожаротушения.

3.1.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИСПДн в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.1.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИСПДн, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

- локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;
- источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);
- резервные линии электропитания в пределах комплекса зданий;
- аварийные электрогенераторы.

3.1.6. Системы обеспечения отказоустойчивости:

- кластеризация;
- технология RAID.

3.1.7. Для обеспечения отказоустойчивости критичных компонентов ИСПДн при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации.

Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИСПДн должны использоваться территориально удаленные системы кластеров.

Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

3.1.8. Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на твердый носитель (ленту, жесткий диск и т.п.).

3.2. Организационные меры

3.2.1. Резервное копирование и хранение данных должно осуществлять на периодической основе:
   - для обрабатываемых персональных данных – не реже раза в неделю;
   - для технологической информации – не реже раза в месяц;
   - эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

3.2.2. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.

3.2.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2.4. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

3.2.5. Носители должны храниться не менее года, для возможности восстановления данных.