«УТВЕРЖДЕНО»
Генеральным директором
ДОУ «ЦРР- детский сад от А до Я»
Кочкаровой Ф.Я.
Приказ №29/1 от 18.09.2017г.

ПОРЯДОК

требования к оборудованию помещений и размещению технических средств, уничтожения, блокирования используемых для обработки персональных данных ДОУ «ЦРР –детский сад от А до Я»

1. Общие положении

1.1. Настоящий Порядок требования к оборудованию помещений и размещению технических средств, уничтожения, блокирования используемых для обработки персональных данных ДОУ «ЦРР –детский сад от А до Я» определяет условия и способы; - порядок требования к оборудованию помещений и размещению технических средств, уничтожения бумажных носителей (документов), содержащих персональные данные, по достижению цели обработки этих персональных данных.

- персональных данных в машинных носителях информации, в том числе персональных данных, и при необходимости самих машинных, носителей информации.

2. Порядок требований к оборудованию помещений и размещению технических средств

• Расположение выделенных помещений и размещаемых в них технических средств должно исключать возможность бесконтрольного проникновения в эти зоны посторонних лиц и гарантировать сохранность находящихся в них конфиденциальных документов, содержащих персональные данные.

• Размещение оборудования и технических средств, предназначенных для обработки персональных данных, должно соответствовать требованиям техники безопасности, санитарным нормам, а также требованиям пожарной безопасности.

• Внутренняя планировка и расположение рабочих мест в выделенных помещениях должны обеспечивать исполнителям сохранность доверенных им конфиденциальных документов и сведений, содержащих персональные данные.

• Входные двери выделенных помещений должны быть оборудованы замками, гарантирующими санкционированный доступ в них в нерабочее время.

• Окна и двери выделенных помещений должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за всеми сигнальными устройствами.

• В выделенные помещения по утвержденному списку допускаются руководство организации, сотрудники службы (*ответственный за*) информационной безопасности, сотрудники информационно - технической службы, иные уполномоченные лица и исполнители, имеющие прямое отношение к приему, обработке и передаче персональных данных.

• Допуск в выделенные помещения вспомогательного и обслуживающего персонала (уборщицы, электромонтеры, сантехники и т.д.) производится только при служебной необходимости и в сопровождении ответственного за помещение, при этом необходимо принять меры, исключающие визуальный просмотр конфиденциальных документов, содержащих персональные данные.

• По окончании рабочего дня выделенные помещения необходимо закрывать и опечатывать, затем их сдают под охрану с указанием времени приема/сдачи и отметкой о включении и выключении охранной сигнализации в журнале приема/сдачи помещений под охрану.

• Сдачу ключей и выделенных помещений под охрану, а также получение ключей и вскрытие выделенных помещений имеют право производить только сотрудники, работающие в этих помещениях и внесенные в утвержденный руководством организации список с образцами подписей этих сотрудников. Список хранится у ответственного дежурного подразделения безопасности.

• Перед вскрытием выделенных помещений должна быть проверена целостность оттисков печатей и исправность замков. При обнаружении нарушения целостности оттисков печатей, повреждения замков или других признаков, указывающих на возможное проникновение в эти помещения посторонних лиц, помещение не вскрывается, а о случившемся немедленно информируется руководство организации и подразделение безопасности (или иное уполномоченное лицо).

• В случае утраты ключа от входной двери выделенного помещения немедленно ставится в известность подразделение безопасности (или иное уполномоченное лицо).

• В выделенных помещениях, где установлены средства защиты информации от утечки по техническим каналам, запрещается приносить и использовать радиотелефоны/сотовые телефоны и другую радиоаппаратуру.

• На случай пожара, аварии или стихийного бедствия должны быть разработаны специальные инструкции, утвержденные руководством организации, в которых предусматривается вызов администрации, должностных лиц, вскрытие выделенных помещений, очередность и порядок спасения конфиденциальных документов, содержащих персональные данные, и дальнейшего их хранения.

3. Блокирование и уничтожение персональных данных, содержащихся в машинных носителях информации

• Блокирование информации, содержащей персональные данные субъекта персональных данных, производится в случаях: если персональные данные являются неполными, устаревшими,

• недостоверными:

• если сведения являются незаконно полученными

• или не являются необходимыми для заявленной оператором персональных данных цели обработки.

• В случае подтверждения факта недостоверности персональных данных уполномоченное Оператором лицо на основании документов, представленных субъектом персональных данных, уполномоченным органом по защите прав субъектов персональных данных или полученных в ходе самостоятельной проверки, обязано уточнять персональные данные и снять их блокирование.

• В случае выявления неправомерных действий с персональными данными уполномоченное Оператором лицо обязано устранить (организовать устранение) допущенные нарушения. В случае невозможности устранения допущенных нарушений необходимо в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными, уничтожить персональные данные.

• Об устранении допущенных нарушений или об уничтожении персональных данных уполномоченное Оператором лице обязано уведомить субъекта персональных данных, а в случае, если обращение или запрос были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган

• Уполномоченное Оператором лицо обязано уничтожить персональные данные субъекта персональных данных в случаях:

• достижения цели обработки персональных данных оператор; отзыва субъектом согласия на обработку своих персональных данных.

• Уничтожение персональных данных должно быть осуществлено в течение трех дней с указанных моментов. В согласии субъекта персональных данных на обработку его персональных данных могут быть установлены иные сроки уничтожения персональных данных при достижении цели обработки персональных данных.

4. Работа с бумажными носителями (документами)

• Виды и периоды уничтожения бумажных носителей, содержащих персональные данные, представлены в таблице 1:

Таблица 1

Виды и периоды уничтожения бумажных носителей, содержащих персональные данные

№ п/п	Документ	Срок хранения	Действия по окончании срока хранения
1	Документы (сведения, содержащие персональные данные о работниках Оператора), переданные и сформированные при трудоустройстве работника	75 лет	Уничтожение
2	Документы о воспитанниках (сведения, содержащие персональные данные воспитанников), родителей (законных представителей)	Установленные для данных документов сроки хранения	Уничтожение
3	Другие документы с грифом «Конфиденциально» и «Для служебного пользования» (Журналы учѐта, списки доступа, эксплуатационная документация и т,п.)	Хранятся до замены на новые, если не указан конкретный срок	Уничтожение

• Документы, указанные в п. 3.1. должны находиться в шкафах с замком, сейфах с доступом к ним сотрудника отдела кадров или уполномоченных лиц. Исключение составляют документы, обрабатываемые в настоящий момент на рабочем месте.

• По окончании срока хранения документы, указанные в п. 3.1 уничтожаются путѐм измельчения на мелкие части (или иным способом), исключающие возможность последующего восстановления информации или сжигаются.

5. Работа с машинными носителями информации

• Виды и периоды уничтожения персональных данных, хранимых в электронном виде («файлах») на жестком диске компьютера (далее - НЖМД) и

машинных носителях: компакт дисках (далее - CD-R/RW, DVD-R/RWв зависимости от формата), FLASH-накопителях.

Таблица 2

Виды и периоды уничтожения персональных данных, хранимых в электронном виде на жестком диске компьютера

№ п/п	Информация, вид носителя	Срок хранения	Действия по окончании срока хранения
1	База данных автоматизированной информационной системы Оператора Носитель: файлы на НЖМД сервера	До создания более актуальной копии	Повторное использование носителя для записи очередной резервной копии БД. в случае невозможности - уничтожение носителя, удаление архивных файлов с НЖМД

• Машинные носители информации (за исключением НЖМД), перечисленные в п.п. 3.1. должны находиться в сейфе, кроме формируемых или обрабатываемых в данный момент на рабочем месте.

• По окончании указанных сроков хранения, машинные носители информации, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путѐм деформирования, нарушения единой целостности носителя или его сжигания.

• Подлежащие уничтожению файлы, расположенные на жестком диске компьютера, удаляются средствами операционной системы с последующим «очищением корзины».

• В случае допустимости повторного использования носителя формата CD-RW, DVD-RW, FLASHприменяется программное удаление («затирание») содержимого диска путѐм его форматирования с последующей записью новой информации на данный носитель.

5. Порядок оформления документов об уничтожении носителей

• Уничтожение носителей, содержащих персональные данные, осуществляет специальная Комиссия, создаваемая приказом руководителя Оператора.

• В ходе процедуры уничтожения персональных данных носителей необходимо присутствие членов Комиссии, осуществляющей уничтожение персональных данных и иной конфиденциальной информации, находящейся на технических средствах.

• Комиссия составляет и подписывает Акт об уничтожении носителей. В течение трѐх дней после составления акты об уничтожении направляются на утверждение руководителю Оператора. После утверждения Акт хранится в сейфе у руководителя соответствующего подразделения Оператора.

• Факт уничтожения носителя с персональными данными фиксируется в «Журнале регистрации носителей информации, содержащих персональные данные и иную конфиденциальную информацию», где в графе «Дата и номер акта

уничтожения» заносятся соответствующие данные. Данный журнал является документом конфиденциального характера и вместе с актами уничтожения хранится в сейфе.

Приложение

А К Т №_____

уничтожения персональных данных и иной конфиденциальной информации, находящейся на технических средствах информационных систем

Комиссия в составе:
Председатель
Члены комиссии

Составили настоящий акт в том, что « ___ » _____ 20_ г. произведено уничтожение персональных данных или иной конфиденциальной информации, находящейся на

№	Информация (наименование документа)	Вид носителя, учѐтный номер	Количество	Примечание

Перечисленные съемные носители уничтожены путем механического уничтожения, сжигания, разрезания, и т.д (нужное подчеркнуть)

Подписи членов комиссии

_____ _____
Ф.И.О. подпись

_____ _____
Ф.И.О. подпись

_____ _____
Ф.И.О. подпись

_____ _____
Ф.И.О. подпись

_____ _____
Ф.И.О. подпись