Утверждаю:

Директор МАУК ДО «Киевская

детская школа искусств»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Д.С.Толстых

«\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024г.

**Регламент**

**резервного копирования и восстановления информации**

**в информационных системах МАУК ДО «Киевская детская школа искусств»**

1. Общие положения

1.1. Регламент резервного копирования и восстановления информации в информационных системах (далее – Регламент) МАУК ДО «Киевская детская школа искусств» (далее – Оператор), разработан в соответствии с требованиями Федерального закона от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07. 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 01.11.2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также иными нормативными правовыми актами регулирующими защиту и обработку персональных данных.

1.2. Регламент разработан для следующих целей:

* определение порядка резервирования информации;
* определения порядка восстановления информации в случае ее искажения или утраты;
* упорядочения работы работников, проводящих резервное копирование и восстановлением информации.

1.3. Регламент определяет действия при выполнении следующих мероприятий:

* резервное копирование;
* контроль резервного копирования;
* хранение резервных копий;
* восстановление информации.

2. Порядок резервного копирования

2.1. Резервному копированию подлежит:

* информация ограниченного доступа, в том числе содержащая персональные данные (далее – ПДн), хранящаяся на сервере Оператора;
* информация ограниченного доступа, в том числе содержащая ПДн, хранящаяся на автоматизированных рабочих местах (далее - АРМ) Оператора.

2.2. Резервное копирование/восстановление информации осуществляется штатными средствами операционных систем с использованием программного обеспечения Оператора администратором информационной безопасности по мере необходимости.

2.3. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) носителей резервных копий без потерь информации, а также обеспечивать восстановление информации в случае отказа любого из устройств резервного копирования.

2.4. Резервное копирование/восстановление информации, хранящейся на АРМ, осуществляется на учтенные съемные носители.

2.5. Необходимость и периодичность резервного копирования информации, хранящейся на АРМ, а также срок хранения резервных копий определяется администратором информационной безопасности.

2.6. Не допускается создание резервных копий на неучтенные и личные носители информации. При использовании съемных машинных носителей как носителей ПДн запись в журнале учета должна содержать отметку «Конфиденциально».

2.7. Хранение съемных машинных носителей ПДн должно осуществляться в сейфах (металлических шкафах), оборудованных внутренними замками и приспособлениями для опечатывания замочных скважин.

2.8. ПДн, содержащиеся на машинных носителях, которые перестали использоваться в системе резервного копирования, должны уничтожатся в порядке, установленном локальными нормативными актами Оператора.

2.9. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть немедленно сообщено ответственному за организацию обработки персональных данных.

3. Восстановление информации

3.1. Восстановление информации, хранящейся на сервере и АРМ производится администратором информационной безопасности на основании заявки работника, имеющего доступ к АРМ или иного уполномоченного лица.

3.2. В случае повреждения или утраты информации, хранящейся на АРМ до начала восстановления их со съемного носителя, следует определить причину утраты или повреждения файлов, содержащих ПДн.

3.3. Если повреждение или удаление информации вызвано действиями самого пользователя (непреднамеренное удаление файла), восстановление информации со съёмного носителя может осуществляться незамедлительно.

3.4. В случае повреждения файловой системы АРМ или работоспособности жесткого диска в результате системного сбоя АРМ восстановление может быть выполнено только после восстановления работоспособности АРМ.

3.5. В случае повреждения или утраты файлов, содержащих конфиденциальную информацию, в том числе ПДн, вследствие несанкционированного доступа (далее – НСД) к АРМ работник Оператора установивший указанный факт незамедлительно сообщает о нем ответственному за организацию обработки персональных данных и администратору информационной безопасности.

3.6. В случае, предусмотренном п. 3.5. Регламента, восстановление из резервной копии может осуществляться только после проведения расследования инцидента безопасности НСД с соответствующим устранением угрозы дальнейших инцидентов НСД.