Приложение
к Приказу МБУ ДО «Тульская детская
художественная школа им. В.Д. Поленова»
№ 019 от 01.03.2019 г.

РЕГЛАМЕНТ
резервного копирования и восстановления информации в информационных системах ИС-1ТДХШ-20, ИС-2ТДХШ-22.23.29, ИС-3ТДХШ-31 МБУДО «Тульская детская художественная школа им. В.Д. Поленова».

I. Общие положения

1.1. Настоящий Регламент резервного копирования и восстановления информации в информационных системах ИС-1ТДХШ-20, ИС-2ТДХШ-22.23.29, ИС-3ТДХШ-31 МБУДО «Тульская детская художественная школа им. В.Д. Поленова» (далее – регламент), хранящихся на сервере и автоматизированных рабочих местах (далее – АРМ) МБУДО «Тульская детская художественная школа им. В.Д. Поленова» (далее – ТДХШ), разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года № 149 ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 года № 152 ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативных и методических документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

1.2. Настоящий регламент разработан с целью:

- определения порядка резервирования информации;
- определения порядка восстановления информации в случае ее искажения или утраты, в связи с попытками несанкционированного доступа, сбоями или отказами аппаратного, или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);
- упорядочения работы сотрудников, проводящих резервное копирование и восстановлением информации;

1.3. В настоящем Регламенте определены действия при выполнении следующих мероприятий:

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

II. Порядок резервного копирования

2.1. Резервному копированию подлежит информация следующих основных категорий:

- информация ограниченного доступа, в том числе персональные данные (далее – ПДн), хранящаяся на сервере ТДХШ (базы данных, файлы и каталоги);
- информация ограниченного доступа, в том числе ПДн, хранящаяся на АРМ ТДХШ.

2.2. **Резервное копирование/восстановление информации** осуществляется штатными средствами операционных систем с использованием программного обеспечения ТДХШ **специалистом по обслуживанию компьютерной техники ТДХШ** (штатным или нештатным) на основании заявки ответственного за обеспечение безопасности персональных данных в информационной системе (далее – ответственный).

2.3. **Контроль результата** процедур резервного копирования и восстановления информации ограниченного доступа осуществляет ответственный.

2.4. 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.

2.5. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

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

2.7. Необходимость и периодичность резервного копирования информации, хранящейся на АРМ, а также срок хранения резервных копий определяется пользователями самостоятельно.

2.8. 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».

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

2.10. В случае отсутствия сейфа (металлического шкафа) у пользователя, осуществляющего хранение, допускается осуществлять хранение в сейфе ответственного.

2.11. Носители с ПДн, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием программного обеспечения, реализующим полное физическое уничтожение данных.

2.12. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности, произошедших в процессе резервного копирования, должно быть немедленно сообщено ответственному.

III. Восстановление информации из резервной копии.

3.1. **Восстановление информации**, хранящейся на сервере и (или) АРМ производится **специалистом по обслуживанию компьютерной техники ТДХШ (штатным или нештатным)** на основании заявки ответственного.

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 пользователь должен обратиться к ответственному.

Перенос файлов из резервной копии может выполняться 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 пользователь незамедлительно сообщает о данном факте ответственному.

Восстановление файлов из резервной копии может осуществляться только после проведения расследования инцидента безопасности НСД с соответствующим устранением угрозы дальнейших инцидентов НСД.

3.6. Если утрата файлов на АРМ произошла в результате вирусного заражения, восстановление файлов возможно только после выполнения мероприятий в соответствии с инструкцией антивирусной защиты ТДХШ.