Приложение №3

УТВЕРЖДАЮ

Директор школы Маряскина О.В.

Приказ от «19» апреля 2019 № 128

Правила осуществления внутреннего контроля соответствия персональных данных законодательству РФ

1. **Общие положения**

1.1Настоящие Правила осуществления внутреннего контроля соответствия персональных данных законодательству РФ в ГБОУ СОШ № 2 п.г.т. Безенчук (далее - Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством, в том числе Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных".

1.2Правила разработаны с учетом требований Федерального закона от 27.07.2006 N 152ФЗ "О персональных данных", постановления Правительства Российской Федерации от 21.03.2011 N 211 "Об утверждении 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", иных нормативных правовых актов.

2. **Порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям законодательства**

2.1Цель проведения внутреннего контроля состоит в проверке и оценке соответствия обеспечения безопасности персональных данных (далее - ПДн) требованиям действующего законодательства, в том числе Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", политики школы №37 в отношении обработки ПДн.

2.2При проведении контроля используются процедуры документальной проверки, опрос и интервью с работниками школы. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего контроля в качестве дополнительного способа может применяться "проверка на месте", которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования.

2.3При проведении внутреннего контроля должно быть обеспечено документальное и, если это необходимо, техническое подтверждение того, что:

- политика в отношении обработки ПДн соответствует требованиям законодательства Российской Федерации;
- организационная структура обеспечения безопасности ПДн создана;
- процессы выполнения требований безопасности ПДн исполняются и удовлетворяют поставленным целям;
- защитные меры (межсетевые экраны, средства защиты информации от несанкционированного доступа и т.п.) настроены и используются правильно; - остаточные риски безопасности ПДн оценены и остаются приемлемыми; - рекомендации предшествующих проверок реализованы.

2.4. При проведении внутреннего контроля могут использоваться журналы средств защиты информации для выявления попыток несанкционированного доступа к защищаемым ресурсам, а также журнал учета нештатных ситуаций информационных систем персональных данных (далее - ИСПДн), ведущийся лаборантом.

3. **План внутренних проверок режима защиты персональных данных**

N п/п	Мероприятие	Периодичность	Исполнитель
1.	Контроль выполнения требований по режиму доступа в защищаемые помещения и на автоматизированные рабочие места, на которых производится обработка персональных данных	Постоянно	Ответственные работники
2.	Контроль соблюдения правил работы с носителями персональных данных	Постоянно	Ответственные работники
3.	Контроль целостности средств вычислительной техники, используемых для обработки персональных данных. Контроль корректной работы системного и прикладного программного обеспечения, средств защиты информации. Контроль состава технических средств.	Постоянно	Ответственные работники
4.	Контроль за соблюдением режима обработки персональных данных	Постоянно	Ответственные работники
5.	Пересмотр и, при необходимости, корректировка учетных записей пользователей	Еженедельно	Ответственный за АСИОУ
6.	Контроль за выполнением антивирусной защиты, неизменностью настроек средств антивирусной защиты и своевременным обновлением антивирусных баз	Еженедельно	Зам. директора по АХЧ
7.	Контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации	Еженедельно	Ответственное лицо

8.	Контроль за обеспечением резервного копирования, проверка работоспособности резервных копий	Ежемесячно	Ответственный за АСИОУ
9.	Поддержание в актуальном состоянии организационно-распорядительных документов	Ежемесячно	Заместитель директора, ответственный за проведение работы по защите персональных данных
10.	Пересмотр организационно-распорядительной документации, регламентирующей порядок обработки персональных данных и требования по защите персональных данных, с учетом проводимых мероприятий по контролю	Ежегодно По факту изменения целей, технологии или иного значимого аспекта информационной безопасности	Заместитель директора, ответственный за проведение работы по защите персональных данных
11.	Обучение и повышение осведомленности работников в области защиты ПДн	Ежегодно В случае изменения законодательной базы, внутренних нормативных актов в области защиты персональных данных не позднее одного месяца с момента изменений	Заместитель директора, ответственный за проведение работы по защите персональных данных
12.	Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных	Раз в три года	Заместитель директора, ответственный за проведение работы по защите персональных данных
13.	Контроль заведения и удаления учетных записей пользователей	Прием/увольнение работника	Ответственный за АСИОУ