Приложение №1
Утверждена
приказом по МБОУ СОШ с.Кремово
от «31» августа 2017 года № _52

Политика информационной безопасности муниципального бюджетного общеобразовательного учреждения Средней общеобразовательной школы с.Кремово Михайловского муниципального района

1. **Общие положения**

1.1 .Политика информационной безопасности МБОУ СОШ с.Кремово (далее - Школа) определяет цели и задачи системы обеспечения информационной безопасности) и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее-ИБ), которыми руководствуются работники школы при осуществлении своей деятельности.

1.2.Основной целью Политики информационной безопасности школы является защита информации школы при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в управлении.

1.3. Политика информационной безопасности разработана в соответствии с: Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным закон от 10 января 2002г. № 1 -ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №781 от 17.11.07г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». Постановление Правительства РФ №687 от 15.09.08г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» а также рядом иных нормативных правовых актов в сфере защиты информации, Приказ Минкомсвязи России от 16.06.2014 N 161 "Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию"

1.4 Выполнение требований Политики ИБ является обязательным для всех структурных подразделений школы.

1.5.Ответственность за соблюдение информационной безопасности несет каждый сотрудник школы.

2. **Цель и задачи политики информационной безопасности**

2.1.Основными целями политики ИБ являются:

-сохранение конфиденциальности критичных информационных ресурсов; -обеспечение непрерывности доступа к информационным ресурсам школы;

-защита целостности информации с целью поддержания возможности школы по оказанию услуг высокого качества и принятию эффективных управленческих решений;

-повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами школы;

-определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в управлении.

-повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальны угроз ИБ;

-предотвращение и/или снижение ущерба от инцидентов ИБ. 2.2.Основными задачами политики ИБ являются: -разработка требований по обеспечению ИБ;

-контроль выполнения установленных требований по обеспечению ИБ;

-повышение эффективности, непрерывности, контро́лируемости мероприятий по обеспечению и поддержанию ИБ;

-разработка нормативных документов для обеспечения ИБ школы;

-выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ школы;

-организация антивирусной защиты информационных ресурсов школы;

-защита информации школы от несанкционированного доступа (далее- НСД) и утечки по техническим каналам связи; - организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору школы.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ школы направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников школы,

технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2. Наибольшимивозможностями для нанесения ущерба обладает собственный персонал школы. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3. Стратегия обеспечения ИБ школы заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников школы.

4. Основные принципы обеспечения информационной безопасности

4.1.Основными принципами обеспечения ИБ :

-постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов школы;

-своевременное обнаружение проблем, потенциально способных повлиять на ИБ школы, корректировка моделей угроз и нарушителя;

-разработка и внедрение защитных мер;

-контроль эффективности принимаемых защитных мер;

-персонификация и разделение ролей и ответственности между сотрудниками школы за обеспечение ИБ школы исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.0бъекты защиты

-информационный процесс профессиональной деятельности;

-информационные активы школы.

5.2.Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности школы;
- персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации 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;
- другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

6. Требования по информационной безопасности

6.1. В отношении всех собственных информационных активов школы, активов, находящихся под контролем школы, а также активов, используемых для получения доступа к инфраструктуре школы, должна быть определена ответственность соответствующего сотрудника школы.

6.2. Все работы в пределах школы должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в управлении.

6.3. Внос в здание и помещения школы личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш- карты и т.п.), а также вынос их за пределы школы производится только при согласовании с директором школы.

6.4. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну школы и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.5. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вх;од в систему должен осуществляться с использованием уникального имени пользователя и пароля.

6.6. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.7. Доступ третьих лиц к информационным системам школы должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам школы должен быть четко определен, контролируем и защищен.

6.8. Сотрудникам,использующим в работе портативные компьютеры школы, может быть предоставлен удаленный доступ к сетевым ресурсам школы в соответствии с правами в корпоративной информационной системе.

6.9. Сотрудники, имеющие право удаленного доступа к информационным ресурсам школы, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети школы и к каким-либо другим сетям, не принадлежащим школы.

6.10. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети школы, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

6.11. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.
Рекомендованные правила:
- сотрудникам школы разрешается использовать сеть Интернет только в служебных целях;
- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- сотрудники школы не должны использовать сеть Интернет для хранения корпоративных данных; - работа сотрудников школы с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации школы в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем школе;
- сотрудники школы перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть школы для всех лиц, не являющихся сотрудниками школы, включая членов семьи сотрудников школы.
6.12. Директор школы имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.
6.13. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация школы.
6.14. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор.
6.15. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуются "компьютерное оборудование". Компьютерное оборудование является собственностью школы и предназначено для использования исключительно в производственных целях.
6.16. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.
6.17. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:
- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений.
6.18. Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной администратором.
6.19. Сотрудники школы не должны:
- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.
6.20.Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию школы по электронной почте без использования систем шифрования.
6.21. Сотрудники школы для обмена документами должны использовать только свой официальный адрес электронной почты.
6.22. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.
6.23. Не допускается при использования электронной почты:
- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;

- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.24. Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

6.25. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.26. В случае кражи переносного компьютера следует незамедлительно сообщить директору школы.

6.35. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

-проинформировать администратора;

- не пользоваться и не выключать зараженный компьютер;

-не подсоединять этот компьютер к компьютерной сети школы до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором

6.36. Сотрудникам школы запрещается:

- нарушать информационную безопасность и работу сети школы;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;
- передавать информацию о сотрудниках или списки сотрудников школы посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.37.Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.38. Необходиморегулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6.39. Все заявки на проведение технического обслуживания компьютеров должны направляться администратору.

7.Управление информационной безопасностью

7.1.Управление ИБ школы включает в себя:

-разработку и поддержание в актуальном состоянии Политики информационной безопасности;

-разработку и поддержание в актуальном состоянии нормативно- методических документов по обеспечению ИБ ;

-обеспечение бесперебойного функционирования комплекса средств ИБ;

-осуществление контроля (мониторинга) функционирования системы ИБ;

-оценку рисков, связанных с нарушениями ИБ.

8.Реализация политики информационной безопасности

8.1. Реализация Политики ИБ школы осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в управлении.

9. Порядок внесения изменений и дополнений в политику информационной безопасности

9.1.Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

10.Контроль за соблюдением политики информационной безопасности

10.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности школы возлагается на сотрудника, назначенного приказом школы образования.

10.2. Начальник школы образования на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований