УТВЕРЖДЕНО
Директором
МАОУ «СОШ № 32
им. Г.А. Сборщикова» г. Перми
Приказ № 436-уч. от 31 августа 2022
Директор _____ /А.М. Гликсон

ПРАВИЛА
информационной безопасности

1. Общие положения

1.1.Правила информационной безопасности МАОУ «СОШ № 32» г. Перми определяют цели и задачи системы обеспечения информационной безопасности и устанавливают совокупность 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 Правил информационной безопасности является защита информации 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.Правила информационной безопасности разработаны в соответствии с: Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Распоряжением администрации города Перми № 79 от 30.06.2016г., а также рядом иных нормативных правовых актов в сфере защиты информации и являются локальным актом ОО.

1.4.Выполнение требований Правил ИБ является обязательным для всех сотрудников ОО.

2. Цель и задачи Правил информационной безопасности

2.1.Основными целями Правил ИБ являются:

-сохранение конфиденциальности информационных ресурсов;

-обеспечение непрерывности доступа к информационным ресурсам ОО;

-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 ОО;

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

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

-предотвращение и/или снижение ущерба от инцидентов ИБ.

2.2.Основными задачами Правил ИБ являются:

-разработка требований по обеспечению ИБ;

-контроль выполнения установленных требований по обеспечению ИБ;

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

-разработка необходимых нормативных документов для обеспечения ИБ школы;

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

-организация антивирусной защиты информационных ресурсов;

-защита информации от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи;

- организация периодической проверки соблюдения информационной безопасности.

3. Основные принципы обеспечения информационной безопасности

3.1.Основными принципами обеспечения ИБ :

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

-своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность, корректировка моделей угроз и нарушителя;

-разработка и внедрение защитных мер;

-контроль эффективности принимаемых защитных мер;

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

4.Объекты защиты

4.1.Объектами защиты с точки зрения ИБ в управлении являются:

-информационный процесс профессиональной деятельности;

-информационные активы ОО.

4.2.Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности ОО;

- 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 информации

.

5. Требования по информационной безопасности

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

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

5.3.В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

5.4.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 лицам.

5.5. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила работы в сети Интернет:

- 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;

-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;

-запрещается доступ в Интернет через сеть школы для всех лиц, не являющихся сотрудниками школы, включая членов семьи сотрудников.

5.6.Администратор имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

5.7.Сотрудники школы должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация школы.

5.8.Сотрудникам школы запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор локально-вычислительной сети.

5.9.Все компьютерное оборудование (стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящих Правил вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное школой, является ее собственностью и предназначено для использования исключительно в производственных целях.

5.10.Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

5.11.При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

5.12.Все программное обеспечение, установленное на предоставленном школой компьютерном оборудовании, является собственностью школы и должно использоваться исключительно в производственных целях.

5.13.Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника.

5.14.На всех стационарных и портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации.

5.15.Сотрудники школы не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

5.16.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. Строго конфиденциальная информация школы, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

5.17.Сотрудники школы для обмена документами должны использовать только свой официальный адрес электронной почты.

5.18.Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что 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. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.

5.19.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.

5.20.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.

5.21.При возникновении подозрения или выявления наличия вирусов или иных разрушительных компьютерных кодов, сотрудник обязан:

- проинформировать администратора;
- не использовать и не включать 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.

5.22.Сотрудникам школы запрещается:

- нарушать информационную безопасность и работу сети школы;
-получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- передавать информацию о сотрудниках или списки сотрудников школы посторонним лицам;
-создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

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

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

5.25.Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, и согласованы с администратором.

6.Управление информационной безопасностью

6.1.Управление ИБ школы включает в себя:

-разработку и поддержание в актуальном состоянии Правил 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.

7. Реализация Правил информационной безопасности

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

8.Порядок внесения изменений и дополнений в Правила информационной безопасности

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

9.Контроль за соблюдением политики информационной безопасности

9.1.Текущий контроль за соблюдением выполнения требований Политики информационной безопасности школы возлагается на сотрудника, назначенного приказом директора ОО.

9.2.Директор школы на регулярной основе рассматривает реализацию и соблюдение отдельных положений Правил информационной безопасности, а также осуществляет последующий контроль за соблюдением их требований.