Казенное общеобразовательное учреждение
Ханты-Мансийского автономного округа – Югры
«Няганская школа – интернат для обучающихся с ограниченными возможностями здоровья»

СОГЛАСОВАНО
Управляющим советом КОУ «Няганская школа-интернат для обучающихся с ограниченными возможностями здоровья»

(протокол от 31.08.2022 № 13)

УТВЕРЖДАЮ

Приказ от 01.09.2022№ 524

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 032331630008AE78A44A4A9666B69E07AF
Владелец: Сорокина Марина Владимировна
Действителен: с 24.12.2021 до 24.03.2023

Политика информационной безопасности казенного общеобразовательного учреждения Ханты-Мансийского автономного округа – Югры «Няганская школа – интернат для обучающихся с ограниченными возможностями здоровья»

1. Общие положения.

1.1. Политика информационной безопасности казенное общеобразовательное учреждение Ханты-Мансийского автономного округа – Югры «Няганская школа – интернат для обучающихся с ограниченными возможностями здоровья» (далее – образовательная организация) 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 образовательной организации при осуществлении своей деятельности.

1.2.Основной целью Политики информационной безопасности образовательной организации является защита информации образовательной организации 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 (далее – Политика ИБ) разработана в соответствии с: Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных», Указом Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановление Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных,

осуществляемой без использования средств автоматизации», а также рядом иных нормативных правовых актов в сфере защиты информации.
1.4. Выполнение требований Политики ИБ является обязательным для всех структурных подразделений образовательных организаций.
1.5.Ответственность за соблюдение информационной безопасности несет каждый сотрудник образовательной организации.

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 образовательной организации;
- 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 образовательной организации;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в управлении;
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2.Основными задачами политики ИБ являются:

- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка нормативных документов для обеспечения информационной безопасности образовательной организации;
- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности;
- 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 образовательной организации.

3. Концептуальная схема обеспечения информационной безопасности.
3.1. Политика ИБ образовательной организации 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 образовательной организации, 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. Наибольшими возможностями для нанесения ущерба обладает собственный персонал образовательной организации. 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 информационной безопасности образовательной организации заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программное - технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников образовательной организации.

4. Основные принципы обеспечения информационной безопасности.

4.1.Основными принципами обеспечения информационной безопасности:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов образовательной организации;
- своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность образовательной организации, корректировка моделей угроз и нарушителя;
- разработка и внедрение защитных мер;
- контроль эффективности принимаемых защитных мер;
- персонификация и разделение ролей и ответственности между сотрудниками образовательной организации за обеспечение информационной безопасности образовательной организации исходит из принципа персональной и единоличной ответственности за совершаемые операции.

5.Объекты защиты.

5.1. Объектами защиты с точки зрения информационной безопасности в управлении являются:

- информационный процесс профессиональной деятельности;
- информационные активы образовательной организации.

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 образовательной организации, активов, находящихся под контролем образовательной организации, а также активов, используемых для получения доступа к инфраструктуре образовательной организации, должна быть определена ответственность соответствующего сотрудника образовательной организации. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами образовательной организации должна доводиться до сведения директора образовательной организации.

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

6.3. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну образовательной организации и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.
6.4. Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.
6.5. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход 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. В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.
6.8. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

- сотрудникам образовательной организации 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 образовательной организации не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников образовательной организации 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 образовательной организации;
- сотрудники образовательной организации перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть образовательной организации для всех лиц, не являющихся сотрудниками образовательной организации, включая членов семьи сотрудников образовательной организации.

6.9.Администратор (инженер – электроник) имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.
6.10. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация образовательной организации.
6.11. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор (инженер –

электроник).
6.12. 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, предоставленное образовательной организацией, является ее собственностью и предназначено для использования исключительно в производственных целях.
6.13. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.
6.14. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь должен обратиться к администратору (инженеру – электронику). Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.
6.15. Порты передачи данных, в том числе CD дисководы в стационарных компьютерах сотрудников образовательной организации блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись от администратора (инженера – электроника).
6.16. Все программное обеспечение, установленное на предоставленном образовательной организацией компьютерном оборудовании, является собственностью образовательной организации и должно использоваться исключительно в производственных целях.
6.17. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если входе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственно директору образовательной организации.
6.18. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;
- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков.

6.20.Сотрудники образовательной организации не должны:

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

6.21. Все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной администратором (инженером – электроником).
6.22.Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию образовательной организации по электронной почте без использования систем шифрования. Строго конфиденциальная информация образовательной организации, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.23. Использование сотрудниками образовательной организации публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации (инженер – электроник) при условии применения механизмов шифрования.
6.24. Сотрудники образовательной организации для обмена документами должны использовать только свой официальный адрес электронной почты.
6.25. 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. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю.
6.26. 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.

6.27. 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.
6.28. В случае кражи переносного компьютера следует незамедлительно сообщить администратору (инженеру-электронику) и\или директору.
6.29. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать администратора (инженера – электроника);
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети образовательной организации до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором (инженером – электроником).

6.30. Сотрудникам образовательной организации запрещается:

- нарушать информационную безопасность и работу сети образовательной организации;
- 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;

- передавать информацию о сотрудниках или списки сотрудников школы посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.31.Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.
6.32. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.
6.33. Все заявки на проведение технического обслуживания компьютеров должны направляться администратору (инженеру – электронику).
6.34. Список помещений, предназначенных для обработки персональных данных (конфиденциальной информации) утверждается директором образовательной организации.

7. Управление информационной безопасностью

7.1. Управление информационной безопасность образовательной организации включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению информационной безопасности;
- обеспечение бесперебойного функционирования комплекса средств информационной безопасности;
- оценку рисков, связанных с нарушениями информационной безопасности.

8. Реализация политики информационной безопасности

8.1. Реализация Политики информационной безопасности образовательной организации 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 образовательной организации возлагается на сотрудника, назначенного приказом директора образовательной организации.
10.2. Директор образовательной организации на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.