муниципальное бюджетное учреждение дополнительного образования города Новосибирска «Детская школа искусств № 12»
630089, г. Новосибирск, ул. Б.Богаткова, 205 а, тел.(383) тел. 311-04-82, 311-04-96

УТВЕРЖДЕНО:
приказом МБУДО ДШИ № 12
от «09» января 2024г. №14 - ОД

Директор МБУДО ДШИ № 12

М.В. Рогова

ПОЛОЖЕНИЕ
об информационной безопасности муниципального бюджетного учреждения дополнительного образования города Новосибирска «Детская школа искусств № 12»

1. Общие положения

1.1. Положение об информационной безопасности МБУДО ДШИ №12 (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 преподаватели и сотрудники школы (далее - сотрудники) при осуществлении своей деятельности.

1.2. Основной целью Положение об 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. Положение об информационной безопасности разработано в соответствии с: ФЗ от 27.07.2006г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», ФЗ от 27.07.2006г. №152-ФЗ «О персональных данных», Постановлением Правительства РФ №781 от 17.11.2007г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства РФ №687 от 15.09.2008г. «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства РФ от 10.07.2013г. №582 «Об утверждении правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации.

1.4. Выполнение требований Положения об ИБ является обязательным для всех сотрудников школы.

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

2. Цель и задачи Положения об информационной безопасности

2.1. Основными целями положения об ИБ являются:
-сохранение конфиденциальности 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;
-повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;
-предотвращение и/или снижение ущерба от инцидентов ИБ.
2.2. Основными задачами положения об ИБ являются:
-разработка требований по обеспечению ИБ;
-разработка нормативных документов для обеспечения ИБ школы;
-контроль выполнения установленных требований по обеспечению ИБ;
-организация антивирусной защиты информационных ресурсов школы;
-защита информации школы от несанкционированного доступа (далее - НСД) и утечки по техническим каналам связи.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Положение об ИБ школы направлено:
-на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников;
-на 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;
-на обеспечение эффективного и бесперебойного процесса деятельности.
3.2. Наибольшими возможностями для нанесения ущерба обладает собственный персонал школы. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергосбережения 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. Объекты защиты

4.1.Объектами защиты с точки зрения ИБ в управлении являются:
-информационный процесс профессиональной деятельности;
-информационные активы школы
4.2. 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 ФИО, 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».

5. Требования по информационной безопасности

5.1. В отношении всех собственных активов школы, активов, находящихся под контролем школы, должна быть определена ответственность соответствующих сотрудников школы. Информацию о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами школы должна контролироваться ответственными лицами за информационную безопасность школы и доводиться до сведения директора школы.

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

5.3. Административный персонал должен периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

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

5.5. 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.

5.6. 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.

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

5.8. Правила использования сети Интернет в МБУДО ДШИ № 12:

-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 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.

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

5.10. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит программист.

5.11. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (принтеры, сканеры и др.), аксессуары («мышь», дисководы для CD- дисков), коммуникационное оборудование (сетевые адаптеры и др.) для целей настоящее политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное школой, является ее собственностью и предназначено для использования исключительно в производственных целях.

5.12. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.
5.13. 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 программисту или администрации школы. 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.
5.14. 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 не нем информации.
5.15. Все программное обеспечение, установленное на предоставленном школой компьютерном оборудовании, является собственностью школы и должно использоваться исключительно в производственных целях.
5.16. Сотрудникам запрещается устанавливать на представленном в пользование компьютерном оборудовании нестандартное, нелицензированное программное обеспечение или программное обеспечение, не имеющее отношение 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 непосредственно директору школы.
5.17. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:
-персональный межсетевой экран;
-антивирусное программное обеспечение.
5.18. Сотрудники школы не должны:
-блокировать антивирусное программное обеспечение;
-устанавливать другое антивирусное программное обеспечение;
-изменять настройки и конфигурацию антивирусного программного обеспечения.
5.19. 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. Строго конфиденциальная информация школы, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.
5.20. Сотрудники школы для обмена документами должен использовать только официальный адрес электронной почты школы.
5.21. 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.
5.22. Не допускается при использовании 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;
-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.

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

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

5.25. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:
-проинформировать ответственных за ИБ;
-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 программистом.

5.26. Аудио и видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник школы, который отвечает за подготовку заседания, после получения письменного разрешения руководителя.

5.27. 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;
-передавать информацию о сотрудниках или списки сотрудников школы посторонним лицам;
-создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.

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

5.29. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

5.30. Все заявки на проведение технического обслуживания компьютеров должны направляться ответственным за информационную безопасность школы.

6. Управление информационной безопасностью

6.1. Управление ИБ школы включает в себя:
-разработку и поддержание в актуальном состоянии Положения об информационной безопасности;
-разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ;
-обеспечение бесперебойного функционирования комплекса средств ИБ.

7. Порядок внесения изменений и дополнений в Положение об информационной безопасности

7.1. Внесение и дополнение в Положение об информационной безопасности производится с целью приведения в соответствие определенных Положением защитных мер реальным жизненным условиям и текущим требованиям к защите информации по мере необходимости.

8. Контроль за соблюдением Положения об информационной безопасности

8.1. Текущий контроль за соблюдением выполнения требований Положения об информационной безопасности школы возлагается на сотрудников, назначенных приказом директора школы.

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