Министерство науки и высшего образования Республики Казахстан
НАО «Павлодарский педагогический университет им. Ә. Марғұлан»

УТВЕРЖДАЮ
Член правления - проректор
по научной работе
_____ Б.С. Есенгельдин
«28» 11 2023 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ШКОЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

Павлодар, 2023

РАЗРАБОТАНО:

Рабочей группой в рамках проекта AP19678646 «Педагогическое обеспечение кибербезопасности школьной среды с использованием комплаенс-менеджмента».

Руководитель проекта - к.п.н, профессор Ж.О. Жилбаев
Главный научный сотрудник - PhD, ассоциированный профессор Д.Б. Абыкенова
Главный научный сотрудник - д.п.н., профессоор Л.С. Сырымбетова
Ведущий научный сотрудник - к.п.н., профессоор А.Ж. Асаинова
Старший научный сотрудник - Ж.Н. Матенова

СОДЕРЖАНИЕ

1. Общие положения

Информация является ценным и жизненно важным ресурсом средней общеобразовательной школы (далее – Школа). Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Школе.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Школы, обучающийся, при этом первоочередной задачей является обеспечение безопасности всех активов Школы. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Школы. Главные цели Школы не могут быть достигнуты без своевременного и полного обеспечения сотрудников и обучающихся информацией, необходимой им для выполнения своих обязанностей.

В настоящей Политике под термином «сотрудник» понимаются все сотрудники Школы, а под термином «обучающийся» - все обучающиеся Школы. Положения настоящей Политики также распространяются на лиц, работающих в Школы по договорам гражданско-правового характера (совместители), в том числе прикомандированных,

1.1. Цель и назначение настоящей Политики

Целями настоящей Политики являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам Школы для поддержки деятельности;
- защита целостности деловой информации с целью поддержания возможности Школы по оказанию образовательных 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 и обучающихся по обеспечению информационной безопасности в Школе.

Администрация Школы должна обеспечить регулярный контроль за соблюдением положений настоящей Политики. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки.

1.2. Область применения настоящей Политики

Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Школы. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных) и обучающихся.

Школе принадлежит на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные

ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Школы, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала Школы.

2. Требования и рекомендации

2.1. Ответственность за информационные активы

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.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами Школы должна доводиться до сведения администрации Школы.

2.2. Контроль доступа к информационным системам

2.2.1. Общие положения

Все работы в пределах Школы выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Школе.

Внос в здания 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 администрацией Школы.

Все данные (конфиденциальные или строго конфиденциальные), составляющие коммерческую тайну Школы и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. Все портативные компьютеры Школы должны быть оснащены программным обеспечением по шифрованию жесткого диска.

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

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, если работа выполняется дома.

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.

2.2.2. Доступ третьих лиц к системам Школы

Каждый сотрудник обязан немедленно уведомить администрацию Школы обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

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.

2.2.3. Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам Школы с учетом их взаимоотношений со Школой.

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

Сотрудникам, работающим за пределами Школы с использованием компьютера, не принадлежащего Школы, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

Сотрудники и третьи лица, 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 Школе.

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

2.2.4. Доступ к сети Интернет

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

Рекомендованные правила:

- сотрудникам и обучающимся 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 непристойного характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, половой ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;
- сотрудники и обучающиеся Школы не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников и обучающихся Школы с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Школы в сеть Интернет;
- сотрудники и обучающиеся 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.

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

2.3. Защита оборудования

Сотрудники и обучающиеся должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Школы.

Сотрудникам и обучающимся запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят только уполномоченные специалисты после согласования изменений с администрацией Школы.

2.3.1. Аппаратное обеспечение

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 Шкоой, является ее собственностью и предназначено для использования исключительно в производственных целях.

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Школы, обязаны обеспечить их хранение в физически защищенных помещениях, запираемых ящиках рабочего стола, шкафах, или обеспечить их защиту с помощью аналогичного по степени эффективности защитного устройства, в случаях, когда данный компьютер не используется.

Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, как в офисе, так и по месту проживания. В ситуациях, когда возрастает степень риска кражи портативных компьютеров, например, в гостиницах, аэропортах, и т.д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

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 в службу технической поддержки. 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.

При записи какой-либо информации на носитель для передачи его контрагентам или партнерам 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.

Карманные персональные компьютеры, а также мобильные телефоны, имеющие функцию электронной почты и прочие переносные устройства, не относятся к числу устройств, имеющих надежные механизмы защиты данных. В подобном устройстве не рекомендуется хранить конфиденциальную информацию.

Порты передачи данных, в том числе FD и CD дисководы в стационарных компьютерах сотрудников Школы блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись информации у администрации Школы.

2.3.2. Программное обеспечение

Все программное обеспечение, установленное на предоставленном Школой компьютерном оборудовании, является собственностью Школы и должно использоваться исключительно в производственных целях.

Сотрудникам и обучающимся 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 администрации Школы и уполномоченному специалисту.

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.

Все компьютеры, подключенные к корпоративной сети, должны быть оснащены лицензионной системой антивирусной защиты.

Сотрудники Школы не должны:

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

Школа предпочитает приобретать программное обеспечение, а не разрабатывать собственные программы, поэтому пользователям, желающим внедрить новые возможности образовательныхпроцессов, необходимо обсудить свое предложение с администрацией школы, которая

проинформирует их о порядке приобретения и/или разработки программного обеспечения.

2.4. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

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.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте администрации Школы.

Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудники и обучающиеся обязаны:

- проинформировать уполномоченного специалиста и администрацию Школы;
- 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 уполномоченным специалистом.

2.5. Помещения с техническими средствами информационной безопасности

Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

Перечень помещений с техническими средствами информационной безопасности утверждается администрацией Школы.

Участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования с администрацией Школы.

Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник Школы, который отвечает за подготовку заседания, после получения разрешения администрации Школы.

Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

2.6. Управление сетью

Уполномоченные сотрудники и администрация Школы контролируют содержание всех потоков данных проходящих через сеть Школы.

Сотрудникам и обучающимся 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, обучающихся или списки обучающихся посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

2.7 Защита и сохранность данных

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Уполномоченные специалисты и администрация Школы обязаны оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

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

Только уполномоченные специалисты и администрация Школы на основании заявок сотрудников могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

Все заявки на проведение технического обслуживания компьютеров должны направляться уполномоченным специалистам и администрации Школы.

2.8. Разработка систем и управление внесением изменений

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованы с уполномоченными специалистами и администрацией Школы.