Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Акушерский колледж»

Подписано цифровой подписью: Батраков Дмитрий Юрьевич
Дата: 2024.02.06 16:41:44 +03'00'

УТВЕРЖДЕНО
Приказом Директора СПб ГБПОУ «Акушерский колледж»
№ 2 -а от 09.01. 2024года

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СПБ ГБПОУ «АКУШЕРСКИЙ КОЛЛЕДЖ»

г. Санкт Петербург

2024 год

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение предусматривает принятие 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 государственном бюджетном профессиональном образовательном учреждении "Акушерский колледж" (далее – СПБ ГБПОУ «Акушерский колледж».

1.2. Настоящее положение составлено на основании действующего законодательства и нормативных актов:

- Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (с дополнениями изменениями)
- Гражданский кодекс Российской Федерации (часть четвертая, статьи 1225 – 1551)
- Федеральный закон Российской Федерации от 27.07.2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- Федеральный закон Российской Федерации от 27.07 2006 года № 152-ФЗ «О персональных данных».
- Указ Президента от 01.05.2022 «О дополнительных мерах по безопасности Российской Федерации».

1.3. Ответственность за соблюдение информационной безопасности несет каждый работник СПБ ГБПОУ «Акушерский колледж».

1.4. Работники СПБ ГБПОУ «Акушерский колледж» своевременно и в полном объеме обеспечиваются информацией, необходимой им для выполнения своих служебных обязанностей.

1.5. В настоящем Положении термины используются следующем значении: "работник" - это все работники СПБ ГБПОУ «Акушерский колледж». На лиц, работающих в СПБ ГБПОУ «Акушерский колледж» по договорам гражданско-правового характера, положения настоящего Положения распространяются в случае, если это обусловлено в договоре;

"*информационная безопасность*" - это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб работникам и обучающимся СПБ ГБПОУ «Акушерский колледж»;

"*персональный компьютер*" - это компьютер, предназначенный для эксплуатации одним пользователем;

"*удаленный доступ*" - это функция, которая позволяет подключиться к компьютеру через сеть Интернет с любого другого компьютера *(Приложение №1).*

2. ЦЕЛИ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

2.1. Целями настоящего Положения является следующее:

- сохранение конфиденциальности информационных ресурсов;
- обеспечение непрерывного доступа к информационным ресурсам СПБ ГБПОУ «Акушерский колледж» для поддержки деятельности;
- защита целостности деловой информации;
- определение ответственности и обязанностей работников по обеспечению информационной безопасности в СПБ ГБПОУ «Акушерский колледж».

3. ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

3.1. Требования настоящего Положения распространяются на всю информацию и ресурсы обработки информации в СПБ ГБПОУ «Акушерский колледж».

3.2. Соблюдение настоящего Положения обязательно для всех работников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации СПБ ГБПОУ «Акушерский колледж», должна быть оговорена обязанность третьего лица по соблюдению требований настоящего Положения.

3.3. СПБ ГБПОУ «Акушерский колледж» 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, в том числе, на голосовую и факсимильную связь, осуществляемую с использованием оборудования СПБ ГБПОУ «Акушерский колледж», лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и работников.

4. КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

4.1. Все работы в пределах колледжа выполняются в соответствии с должностными обязанностями только на компьютерах, разрешенных к использованию в СПБ ГБПОУ «Акушерский колледж».

4.2. Внос в здания и помещения СПБ ГБПОУ «Акушерский колледж» личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы указанных зданий и помещений производится при согласовании с директором СПБ ГБПОУ «Акушерский колледж».

4.3. Руководители подразделений должны периодически пересматривать права доступа своих работников и других пользователей к соответствующим информационным ресурсам.

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

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

4.6. Руководители подразделений должны обеспечить регулярный контроль за соблюдением настоящего Положения. Кроме того, должна быть организована периодическая проверка соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору СПБ ГБПОУ «Акушерский колледж».

5. ДОСТУП ТРЕТЬИХ ЛИЦ К СИСТЕМАМ

5.1. Каждый работник обязан немедленно уведомить директора СПБ ГБПОУ «Акушерский колледж» обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети. Доступ третьих лиц к информационным системам центра должен быть обусловлен производственной необходимостью.

6. УДАЛЕННЫЙ ДОСТУП

6.1. Пользователи (работники) получают право удаленного доступа к информационным ресурсам СПБ ГБПОУ «Акушерский колледж» с учетом их взаимоотношений с СПБ ГБПОУ «Акушерский колледж» на основании служебной записки согласованной директором СПБ ГБПОУ «Акушерский колледж».

6.2. Работникам, использующим в работе портативные компьютеры СПБ ГБПОУ «Акушерский колледж», может быть предоставлен удаленный

доступ к сетевым ресурсам СПБ ГБПОУ «Акушерский колледж» в соответствии с правами в корпоративной информационной системе.

6.3. Работникам СПБ ГБПОУ «Акушерский колледж», работающим за пределами СПБ ГБПОУ «Акушерский колледж» с использованием компьютера, не принадлежащего СПБ ГБПОУ «Акушерский колледж», запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

6.4. Работники СПБ ГБПОУ «Акушерский колледж», имеющие право удаленного доступа к информационным ресурсам, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети СПБ ГБПОУ «Акушерский колледж» и к каким-либо другим сетям, не принадлежащим СПБ ГБПОУ «Акушерский колледж».

6.5. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети СПБ ГБПОУ «Акушерский колледж», должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

7. ДОСТУП К СЕТИ ИНТЕРНЕТ

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

7.2. Работникам СПБ ГБПОУ «Акушерский колледж» разрешается использовать сеть Интернет только в служебных целях.

7.3. Работникам СПБ ГБПОУ «Акушерский колледж» запрещается посещение развлекательных сайтов, 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.

7.4. Работники СПБ ГБПОУ «Акушерский колледж» не должны использовать сеть Интернет для хранения корпоративных данных.

7.5. Работники СПБ ГБПОУ «Акушерский колледж» при работе с Интернет-ресурсами должны пользоваться только режимом просмотра информации, исключая возможность передачи информации в сеть Интернет.

7.6. Работникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем СПБ ГБПОУ «Акушерский колледж».
7.7. Работники СПБ ГБПОУ «Акушерский колледж» перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов.
7.8. Запрещен доступ в сеть Интернет через сеть СПБ ГБПОУ «Акушерский колледж» для всех лиц, не являющихся работниками СПБ ГБПОУ «Акушерский колледж», включая членов семьи работников.
7.9. Руководство СПБ ГБПОУ «Акушерский колледж» имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

8. ЗАЩИТА ОБОРУДОВАНИЯ

8.1. Работники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация.
8.2. Работникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит специалист по информационным технологиям, после согласования изменений с руководством.

9. АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

9.1. Все компьютерное оборудование (серверы, стационарные и портативные компьютеры и прочее), периферийное оборудование (принтеры, сканеры и прочее), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков и прочее), коммуникационное оборудование (факс-модемы, сетевые адаптеры, концентраторы и прочее) для целей настоящего Положения вместе именуются "компьютерное оборудование". Компьютерное оборудование СПБ ГБПОУ «Акушерский колледж» является его собственностью и предназначено для использования исключительно в производственных целях.
9.2. Каждый работник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности, а также содержащейся в нем информации.

9.3. Все компьютеры должны защищаться паролем при загрузке системы. Для установки режимов защиты пользователь должен обратиться в отдел информационных технологий.

9.4. 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.

9.5. При получении какой-либо информации от третьих лиц на внешний носитель необходимо убедиться в том, что носитель чист, то есть не содержит информации.

10. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

10.1. Все программное обеспечение, установленное на предоставленном СПБ ГБПОУ «Акушерский колледж» компьютерном оборудовании, является его собственностью и должно использоваться исключительно в производственных целях.

10.2. Работникам СПБ ГБПОУ «Акушерский колледж» запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их должностным обязанностям. Если в ходе выполнения технического обслуживания будет обнаружено неразрешенное к установке программное обеспечение, оно будет удалено с сообщением директору СПБ ГБПОУ «Акушерский колледж» о допущенном нарушении.

10.3. На всех компьютерах должно быть установлено антивирусное программное обеспечение.

10.4. Работники СПБ ГБПОУ «Акушерский колледж» не должны:

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

11. ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

11.1. Содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

11.2. Использование электронной почты СПБ ГБПОУ «Акушерский колледж» в личных целях не допускается.
11.3. Работникам СПБ ГБПОУ «Акушерский колледж» запрещается направлять конфиденциальную информацию СПБ ГБПОУ «Акушерский колледж» по электронной почте.
11.4. Работникам СПБ ГБПОУ «Акушерский колледж» запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.
11.5. Работники СПБ ГБПОУ «Акушерский колледж» для обмена документами с деловыми партнерами должны использовать только свой официальный адрес электронной почты. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма, и факсимильные сообщения.
11.6. В целях предотвращения ошибок при отправке сообщений работники СПБ ГБПОУ «Акушерский колледж» 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. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать директора СПБ ГБПОУ «Акушерский колледж».
11.7. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

12. СООБЩЕНИЕ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАГИРОВАНИЕ И ОТЧЕТНОСТЬ

12.1. Работники СПБ ГБПОУ «Акушерский колледж» должны сообщать об известных или подозреваемых ими нарушениях информационной безопасности.
12.2. Работники СПБ ГБПОУ «Акушерский колледж», ни при каких обстоятельствах не должны пытаться использовать ставшие им известными слабые стороны системы информационной безопасности.
12.3. В случае кражи переносного компьютера следует незамедлительно сообщить об этом директору СПБ ГБПОУ «Акушерский колледж».

12.4. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения работник СПБ ГБПОУ «Акушерский колледж» обязан:
- проинформировать специалиста по информационным технологиям;
- не использовать и не выключать зараженный компьютер до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование.

13. УПРАВЛЕНИЕ СЕТЬЮ

13.1. Уполномоченный работник по информационной безопасности контролирует содержание всех потоков данных проходящих через сеть СПБ ГБПОУ «Акушерский колледж».

13.2. Работникам СПБ ГБПОУ «Акушерский колледж» запрещается:
- нарушать информационную безопасность и работу сети;
- 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 работниках, обучающихся, абитуриентах СПБ ГБПОУ «Акушерский колледж» посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочее разрушительное программное обеспечение.

14. ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

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

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

14.3. Специалист по информационной безопасности обязан оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

14.4. Специалист по информационной безопасности на основании заявок руководителей подразделений создает и удаляет совместно используемые сетевые ресурсы и папки общего пользования, а также управляет полномочиями доступа к ним.

14.5. Работники имеют право создавать, модифицировать и удалять файлы 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.

14.6. Все заявки на проведение технического обслуживания компьютеров должны направляться специалистам в службу автоматизированных систем управления.

15. РАЗРАБОТКА СИСТЕМ И УПРАВЛЕНИЕ ВНЕСЕНИЕМ ИЗМЕНЕНИЙ

15.1. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть согласованны с директором СПБ ГБПОУ «Акушерский колледж».

ПРИЛОЖЕНИЕ №1

Служебная записка

Прошу Вас согласовать получение удаленного доступа к ресурсам информационно-телекоммуникационной сети СПБ ГБПОУ «АК» (далее - ИТС) для работы в ней вне учреждения (удаленно).

Обязуюсь строго соблюдать принципы информационной и технической безопасности при работе в ИТС, такие как:

- по окончании работы отключаться от ИТС;

- при работе с ИТС не допускать к монитору третьих лиц;

- не разглашать устно или письменно процесс и результаты работы;

- не передавать третьим лицам ни в устной, ни в письменной, ни в форме электронных сообщений данные настроек программы для подключения ИТС;

- не передавать третьим лицам логин и пароль для доступа к ИТС;

- осуществлять подключение к ИТС со своего личного компьютера или ноутбука.

Я в полной мере ознакомлен (а) о применяемых мерах ответственности за распространение персональных данных, а именно:

Статья 13.11 Ко АП РФ «Нарушение порядка сбора, хранения, использования или распространения персональных данных»;

Статья 238 ТК РФ «Нарушение правил хранения и использования персональных данных, повлекшее за собой материальный ущерб работодателю»;

Статья 243 ТК РФ «Случаи полной материальной ответственности» (п. 7 - Разглашение служебной тайны, ставшей известной работнику при выполнении им трудовых обязанностей»);

Статья 274 УК РФ «Нарушение правил эксплуатации хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»

Я предупрежден(а) о том, что в случае разглашения мной сведений, касающихся персональных данных работников, обучающихся и абитуриентов СПБ ГБПОУ «АК», а также любой иной информации содержащейся в ИТС или их утраты я несу гражданско-правовую, административную и уголовную ответственность в порядке, установленном федеральными в соответствии с ст.90 ТК РФ.

«____» _____ 2024 г. (подпись) (ФИО) (наименование должности, ФИО)