УТВЕРЖДАЮ:

Директор БУ СО ВО

«КЦСОН Великоустюгского района»

_____А.С. Шушарина

«11» января 2021 года

ПОЛОЖЕНИЕ «ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БУ СО ВО «КЦСОН Великоустюгского района»

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее положение информационной безопасности 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 БУ СО ВО «КЦСОН Великоустюгского района» (в тексте допустимо - организация).

Ответственность за соблюдение информационной безопасности несет каждый сотрудник, при этом первоочередной задачей является обеспечение безопасности персональных данных работников и получателей услуг. Главные цели БУ СО ВО «КЦСОН Великоустюгского раойна» не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

В настоящем Положении под терминами:

"сотрудник" понимаются все сотрудники БУ СО ВО «КЦСОН Великоустюгского района». На лиц, работающих в БУ СО ВО «КЦСОН Великоустюгского района» по договорам гражданско-правового характера, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре;

«информационная безопасность» понимается защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб сотрудникам и получателям услуг БУ СО ВО «КЦСОН Великоустюгского района»;

«персональный компьютер» понимается компьютер, предназначенный для эксплуатации одним пользователем;

«удаленный доступ» понимается функция, которая позволяет подключиться к компьютеру через Интернет с любого другого компьютера.

2. ЦЕЛЬ И НАЗНАЧЕНИЕ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

- сохранение конфиденциальности информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам организации для поддержки деятельности;
- защита целостности информации с целью поддержания возможности организации оказания услуг высокого качества и принятию эффективных управленческих решений;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в организации.

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.

3.ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

Требования настоящего Положения распространяются на всю информацию и ресурсы обработки информации в организации. Соблюдение настоящего Положения обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации организации, должна быть оговорена обязанность третьего лица по соблюдению требований настоящего Положения.

4. КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

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

Внос в здания и помещения организации личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы центра производится только при согласовании с директором.

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

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.

5.ДОСТУП ТРЕТЬИХ ЛИЦ К СИСТЕМАМ ОРГАНИЗАЦИИ

Каждый сотрудник обязан немедленно уведомить директора обо всех случаях предоставления доступа третьим лицам к ресурсам сети организации. Доступ третьих лиц к информационным системам центра должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам должен быть четко определен, контролируем и защищен.

6.УДАЛЕННЫЙ ДОСТУП

Пользователи получают право удаленного доступа к информационным ресурсам организации с учетом их взаимоотношений с организацией.

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

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

Сотрудники, имеющие право удаленного доступа к информационным ресурсам, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети центра и к каким-либо другим сетям, не принадлежащим организации.

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

7.ДОСТУП К СЕТИ ИНТЕРНЕТ

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

Рекомендованные правила:

- сотрудникам организации разрешается использовать сеть Интернет только в служебных целях;
- 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;
- сотрудники организации при работе с Интернет-ресурсами должны пользоваться только режимом просмотра информации, исключая возможность передачи информации в сеть Интернет;
- сотрудники организации перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть организации для всех лиц, не являющихся сотрудниками организации, включая членов семьи сотрудников.
- руководство организации имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

8.ЗАЩИТА ОБОРУДОВАНИЯ

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

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит специалист по информационным технологиям, после согласования изменений с руководством.

9.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 настоящего Положения вместе именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное организации, предназначено для использования исключительно в производственных целях.

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

Все компьютеры должны защищаться паролем при загрузке системы. 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.

10.ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

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 директору организации.

11.РЕКОМЕНДУЕМЫЕ ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

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

Использование электронной почты в личных целях не допускается.

Сотрудникам запрещается направлять партнерам конфиденциальную информацию организации по электронной почте.

Сотрудники организации для обмена документами с 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.

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.

Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

Ниже перечислены недопустимые действия и случаи использования электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- групповая рассылка всем пользователям организации сообщений/писем;
- рассылка рекламных материалов, не связанных с деятельностью организации;
- 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 этическим нормам.

Ко всем исходящим сообщениям, направляемым внешним пользователям, пользователь может добавлять уведомление о конфиденциальности.

Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в организации процедурами документооборота.

12.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 информационной безопасности.

В случае кражи переносного компьютера следует незамедлительно сообщить об инциденте директору.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник организации обязан:

- проинформировать специалиста по информационным технологиям;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети организации до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование.

13.ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Специалист по информационным технологиям обязан оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

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

Только специалист по информационным технологиям на основании заявок руководителей подразделений и согласования с директором может 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 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 специалисту по информационным технологиям.

14.РАЗРАБОТКА СИСТЕМ И УПРАВЛЕНИЕ ВНЕСЕНИЕМ ИЗМЕНЕНИЙ

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть согласованны с директором организации.