Приложение №16
к приказу №50/1-ф от 21.07 2016 г.

УТВЕРЖДАЮ

Генеральный директор
ОАО «Новая Поликлиника-Астрахань»

_____ Сидоров Г.А.

«___» _____ 20__ г.

ПОЛИТИКА
информационной безопасности
ОАО «Новая Поликлиника-Астрахань»

1. Общие положения

Информация является ценным и жизненно важным ресурсом ОАО «Новая Поликлиника-Астрахань» (далее – Компания). 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 Компании. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Компании, при этом первоочередной задачей является обеспечение безопасности всех активов Компании. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Компании. Главные цели Компании не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

В настоящей Политике под термином «сотрудник» понимаются все сотрудники Компании. На лиц, работающих в Компании по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

1.1. Цель и назначение настоящей Политики

Целями настоящей Политики являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам Компании для поддержки бизнес деятельности;
- защита целостности деловой информации с целью поддержания возможности Компании по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Компании;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Компании.

Руководители подразделений Компании должны 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 Руководству.

1.2. Область применения настоящей Политики

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

Компании 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 Компании, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала Компании.

2. Требования и рекомендации

2.1. Ответственность за информационные активы

В отношении всех собственных информационных активов Компании, активов, находящихся под контролем Компании, а также активов, используемых для получения доступа к инфраструктуре Компании, должна быть определена ответственность соответствующего сотрудника Компании.

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами Компании должна доводиться до сведения руководителя Департамента информационных технологий и руководителя Департамента защиты информации Компании.

2.2. Контроль доступа к информационным системам

2.2.1. Общие положения

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

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

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

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.

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 Компании

Каждый сотрудник обязан немедленно уведомить руководителя Департамента информационных технологий и руководителя Департамента защиты информации обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

Доступ третьих лиц к информационным системам Компании должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Компании должен быть четко определен, контролируем и защищен.

2.2.3. Удаленный доступ

Пользователи получают право удаленного доступа к информационным ресурсам Компании с учетом их взаимоотношений с Компанией.

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

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

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

Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Компании, 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 Компании 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 Компании не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников Компании с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Компании в сеть Интернет;

- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем Компании;
- сотрудники Компании перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть Компании для всех лиц, не являющихся сотрудниками Компании, включая членов семьи сотрудников Компании.

Специалисты Департамента информационных технологий и Департамента защиты информации имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

2.3. Защита оборудования

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

Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят авторизованные специалисты Департамента информационных технологий, после согласования изменений с Департаментом защиты информации.

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

Пользователи портативных компьютеров, содержащих информацию, составляющую коммерческую тайну Компании, 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, в офисах деловых партнеров и т.д., пользователи обязаны ни при каких обстоятельств не оставлять их без присмотра.

Во время поездки в автомобиле портативный компьютер должен находиться в багажнике. На ночь его следует перенести из автомобиля в гостиничный номер.

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 по бизнесу 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 Компании блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись информации у Департамента защиты информации.

2.3.2. Программное обеспечение

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

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 непосредственному руководителю сотрудника и в Департамент защиты информации.

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 системой антивирусной защиты, утвержденной руководителем Департамента информационных технологий.

Сотрудники Компании не должны:

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

Компания предпочитает приобретать программное обеспечение, а не разрабатывать собственные программы, поэтому пользователям, желающим внедрить новые возможности бизнес-процессов, необходимо обсудить свое предложение со своим менеджером по бизнес информации, который проинформирует их о порядке приобретения и/или разработки программного обеспечения.

2.4. Рекомендуемые правила пользования электронной почтой

Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами или конкурентами по бизнесу для их использования в качестве доказательств в процессе судебного разбирательства или при ведении бизнеса. Поэтому содержание электронных сообщений должно строго соответствовать корпоративным стандартам в области деловой этики.

Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует бизнес деятельности.

Сотрудникам запрещается направлять партнерам конфиденциальную информацию Компании по электронной почте без использования систем шифрования. Строго конфиденциальная информация Компании, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

Сотрудникам Компании запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

Использование сотрудниками Компании публичных почтовых ящиков электронной почты осуществляется только при согласовании с Департаментом защиты информации при условии применения механизмов шифрования.

Сотрудники Компании для обмена документами с бизнес 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. 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. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать специалистов Департамента защиты информации.

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 Компании сообщений/писем;
- рассылка рекламных материалов, не связанных с деятельностью Компании;
- 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 корпоративным стандартам в области этики.

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 Компании процедурами документооборота.

Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры Компании для других пользователей. Объем вложений не должен превышать 2 Мбайт.

2.5. 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 директору Департамента защиты информации.

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 сотрудник обязан:

- проинформировать специалистов Департамента информационных технологий;
- не пользоваться и не выключать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети Компании до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами Департамента информационных технологий.

2.6. 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 Руководством Компании.

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

Аудио/видео запись, фотографирование во время конфиденциальных заседаний может вести только сотрудник Компании, который отвечает за подготовку заседания, после получения письменного разрешения руководителя группы организации встречи.

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

2.7. Управление сетью

Уполномоченные сотрудники Департамента информационных технологий и Департамента защиты информации контролируют содержание всех потоков данных проходящих через сеть Компании.

Сотрудникам Компании запрещается:

- нарушать информационную безопасность и работу сети Компании;

- 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 Компании посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

2.7.1. Защита и сохранность данных

Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях. Специалисты Департамента информационных технологий 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 специалисты Департамента информационных технологий на основании заявок руководителей подразделений 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 в Департамент информационных технологий.

2.8. Разработка систем и управление внесением изменений

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы, согласованны с руководителями Департамента защиты информации и Департамента информационных технологий.