ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ

«КЛИНИКА ЕК»

ИНН 6500012284/КПП 650001001/ОГРН 1236500004916
Адрес: 693004, г. Южно-Сахалинск, Больничная, д. 51, оф. 46-49

ПРИКАЗ № 4 от 05.01.2026 г.

О реструктуризации системы информационной безопасности

В целях обеспечения реструктуризации системы информационной безопасности**,** эффективности работы всех технических и информационных систем ООО «КЛИНИКА ЕК».

ПРИКАЗЫВАЮ:

1. Управляющей клиники:

• Организовать проведение инвентаризации всех имеющихся информационных активов ООО «КЛИНИКА ЕК», классифицировать информационные активы по степени важности, согласовать с генеральным директором - пользователей корпоративной сети, имеющие доступ к каждому конкретному классу информационных активов ООО «КЛИНИКА ЕК», определить способы и объем доступа пользователей к информации (просмотр, изменение, удаление).

1.2. Организовать ежедневное резервное копирование служебной информации в соответствии с утвержденной схемой.

1.3. Установить на рабочих столах пользователей доступ к медицинским сайтам, необходимым для работы.

1.4. Доступ к просмотру не медицинских сайтов, социальным сетям заблокировать.

1.5. 1 раз в неделю проверять историю работы в браузерах сотрудников центра с докладом о работе не с медицинскими сайтами директору.

1.6. Регулярно контролировать объем внешнего трафика, потребляемый каждым сетевым устройством (персональными компьютерами, коммутаторами, серверами и аналогичным оборудованием). При выявлении фактов нецелевого использования доступа к внешним ресурсам осуществлять блокирование объекта, потребляющего трафик, доложить письменно - Генеральному Директору.

1.7. По каждому случаю проводить служебное расследование по фактам нецелевого использования.

1.8. Организовать блокирование доступа к использованию врачами специалистами дискет, CD и DVD RW, USB-накопителей и аналогичных устройств, за исключением применения дисков CD и DVD RW специалистами согласно списка, утвержденного директора.

1.9. Осуществлять постоянную антивирусную проверку программного обеспечения, установленного на клиентских компьютерах, серверах и маршрутизаторах, своевременно обновлять базы вирусных сигнатур. В случае обнаружения вирусных программ на каких-либо объектах локальной вычислительной сети действовать в соответствии с политикой информационной безопасности.

1.10. Регулярно контролировать объем внешнего трафика, потребляемый каждым сетевым устройством (персональными компьютерами, коммутаторами, серверами и аналогичным оборудованием). При выявлении фактов нецелевого использования доступа к внешним

ресурсам осуществлять блокирование объекта, потребляющего трафик, и силами ОИТ проводить служебное расследование по фактам такого использования.
1.11. На рабочих местах пользователей технически обеспечить возможность выполнения только безусловно необходимых для повседневной работы программ, выполнение остальных программ запретить. Предоставить врачам право изменять списки используемых программ только после письменного согласования с главным врачом.
1.12. Осуществлять постоянную антивирусную проверку программного обеспечения, установленного на клиентских компьютерах, серверах и маршрутизаторах, своевременно обновлять базы вирусных сигнатур. В случае обнаружения вирусных программ на каких-либо объектах локальной вычислительной сети действовать в соответствии с политикой информационной безопасности.
1.13. Регламентировать доступ отдельных пользователей и групп пользователей к внешним по отношению к корпоративной сети ресурсам исключительно непосредственной служебной необходимостью, только для работы с медицинскими сайтами и медицинскими базами данных Минздрава РФ, Минздрава Хабаровского края, электронными медицинскими библиотеками, МКБ-10, электронными журналами по специальности.
1.14. Минимизировать внешний по отношению к корпоративной сети трафик. Для расширения количества сайтов, необходимых для работы предоставлять доступ в Интернет только по письменной заявке медицинского персонала. Подачу заявки осуществлять в произвольной форме.
1.15. Взаимодействие серверов и пользовательских компьютеров с внешними по отношению к корпоративной сети ООО «КЛИНИКА ЕК» ресурсами осуществлять только через сконфигурированные специальным образом программно-аппаратные шлюзы.
1.16. Производить анализ проходящего трафика на корректность и наличие злонамеренного программного обеспечения.
1.17. Произвести аудит имеющегося программного обеспечения на предмет наличия необходимого количества лицензий.
1.18. Осуществлять постоянную антивирусную проверку программного обеспечения, установленного на клиентских компьютерах, серверах и маршрутизаторах, своевременно обновлять базы вирусных сигнатур. В случае обнаружения вирусных программ на каких-либо объектах локальной вычислительной сети действовать в соответствии с политикой информационной безопасности.
1.19. При обнаружении невыполнения сотрудниками ООО «КЛИНИКА ЕК» требований немедленно выполнять отключение персонального компьютера от корпоративной сети и ставить в известность генерального директора.
2. Персоналу ООО «КЛИНИКА ЕК»:
2.1. Исключить хранение служебной информации, персональных данных пациентов и сотрудников на локальных устройствах хранения информации клиентских компьютеров, всю необходимую информацию хранить на специально выделенных для этого разделах файловых серверов.
2.2. Не допускать использования внешних аппаратных устройств хранения информации (дискет, CD и DVD RW, USB-накопителей и аналогичных устройств), иначе как по заявке, представленной на имя директора с обоснованием необходимости использования. Подачу заявки осуществлять в произвольной форме.
2.3. Регламентировать установку и использование средств электронных коммуникаций (электронных почтовых ящиков, систем мгновенного обмена сообщениями). Не допускать использование на рабочих местах корпоративной сети почтовых ящиков, находящихся на бесплатных почтовых серверах, а также почтовых ящиков, не обслуживаемых почтовыми серверами ООО «КЛИНИКА ЕК». Предусматривать установку и использование средств электронных коммуникаций только по письменной заявке, в котором будет использованы данные средства.

2.4. Взаимодействие серверов и пользовательских компьютеров с внешними по отношению к корпоративной сети ООО «КЛИНИКА ЕК» ресурсами осуществлять только через сконфигурированные специальным образом программно-аппаратные шлюзы.
3. Для осуществления сетевого управления, хранения данных, работы со служебной информацией, удаленного администрирования пользователей, при равных функциональных возможностях к использовать преимущественно программное обеспечение с открытым кодом, распространяющееся по лицензиям GPL, либо программные продукты, распространяющиеся бесплатно.
4. На рабочих местах пользователей работать только с безусловно необходимыми для повседневной работы программами, выполнение остальных программ запретить.
5. Управляющей клиники не реже одного раза в квартал представлять Генеральному Директору отчет о состоянии информационной безопасности сетей и систем ООО «КЛИНИКА ЕК».
6. В случае возникновения связанных с информационной безопасностью инцидентов глобального характера обязать весь персонал незамедлительно ставить руководство в известность о данных инцидентах.
7. В обязательном порядке довести под роспись до всех сотрудников ООО «КЛИНИКА ЕК» данный приказ и должностную инструкцию по использованию информационных и технических систем ООО «КЛИНИКА ЕК».
8. Контроль исполнения приказа возлагаю на себя.

Генеральный Директор Козинцова Е.Ю.

Приложение № 1
к Приказу № --- от --.01.2026г

Должностная инструкция по использованию
технических и информационных систем ООО «КЛИНИКА ЕК»

Как сотрудник ООО «КЛИНИКА ЕК», использующий персональный компьютер, информационные и технические системы ООО «КЛИНИКА ЕК» в процессе работы, я,_____
ознакомлен(а) с порядком использования информационных и технических систем, за исключением случаев, когда есть вероятность причинения вреда здоровью сотрудников или порчи оборудования, обязуюсь соблюдать следующие правила:

- Доступ в глобальную сеть Интернет, к почтовым, файловым и иным серверам и службам, к любым внешним и внутренним ресурсам организации для всех пользователей информационных систем и сетей ООО «КЛИНИКА ЕК» запрещен за исключением случаев, вызванных служебной необходимостью, по согласованию с директором и в соответствии с утвержденным им списком.

2. Использование электронных почтовых ящиков, находящихся на бесплатных почтовых серверах или на коммерческих почтовых серверах, не принадлежащих ООО «КЛИНИКА ЕК» - **запрещено**. Использование служебных почтовых ящиков, находящихся на почтовых серверах Предприятия, предусмотрено при наличии служебной необходимости.
3. Самостоятельная установка, копирование, распространение и запуск любого программного обеспечения, кроме уже установленного на персональных компьютерах - **запрещена.**
4. Самостоятельная установка какого-либо аппаратного обеспечения (плат расширения, дополнительных модулей, дисководов, картриджей и т.п.) в персональные компьютеры, оргтехнику и иные устройства -**запрещена**. Самостоятельное подключение к персональным компьютерам каких-либо внешних устройств (сотовых и мобильных телефонов, цифровых фотоаппаратов, адаптеров беспроводной связи и иных) - **запрещено.**
5. Самостоятельное перемещение и вскрытие персональных компьютеров, оргтехники и иных аппаратных устройств - **запрещено.** Удаление пломб и инвентарных номеров с персональных компьютеров, оргтехники и иных аппаратных устройств - **запрещено.**
6. Пароли доступа к персональному компьютеру, к электронным почтовым ящикам, к биллинговым, расчетным и торговым программам, к бухгалтерским системам и к любым другим прикладным программам и файлам являются личным идентификатором пользователя в соответствующих информационных подсистемах, и не подлежат разглашению кому бы то ни было, за исключением генерального директора и управляющей. Запись паролей на общедоступных носителях (приклеенных к монитору листах бумаги и т.п.) - **запрещена**. Использование паролей других пользователей для доступа к информационным ресурсам **категорически запрещено**. В случае утраты пароля пользователь должен поставить в известность управляющую клиники.
7. Использование любых внешних и дополнительных внутренних накопителей (дискеты, электронные, оптические и магнитооптические диски), а также модемов и других устройств дистанционной связи, за исключением специально оговоренных случаев - **запрещено.**
8. Хранение на служебных информационных носителях (накопителях на жестких магнитных дисках, встроенных в персональный компьютер, дискетах, носителях CD/DVD-R/RW) личной информации, а также информации, не имеющей отношения к производственной деятельности (музыкальные файлы, фоновые изображения и прочее) - **запрещено.**
9. Вся служебная информация должна храниться на выделенных для этого разделах файловых серверов.
10. Любые виды доступа, включая доступ в Интернет и к любым внешним и внутренним информационным ресурсам, предоставляются по письменной заявке, направляемой сотрудником ООО «КЛИНИКА ЕК» генеральному директору.
11. Каждый пользователь информационной системы ООО «КЛИНИКА НК» **несет личную ответственность за соблюдение данных правил и требований.** Руководители несут ответственность за соблюдение сотрудниками данных правил и требований. Несоблюдение данных правил и требований влечет за собой меры административного воздействия вплоть до увольнения.

Технический смысл всех вышеперечисленных правил мне разъяснен. Возражений не имею.

_____ _____
(число) (подпись)