

# ПОЛОЖЕНИЕ «ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ООО «МЕДИЦИНСКИЙ ЦЕНТР «ЛАЗЕР»»

## 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 ООО «Медицинский центр «Мой доктор».

Ответственность за соблюдение информационной безопасности несет каждый сотрудник, при этом первоочередной задачей является обеспечение безопасности персональных данных работников и пациентов. Главные цели «Медицинский центр «Лазер» 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 «Медицинский центр «Лазер»;

«информационная безопасность» понимается защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб сотрудникам и пациентам ООО «Медицинский центр «Лазер»;

«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 ООО «Медицинский центр «Лазер» для поддержки бизнес деятельности;
- защита целостности деловой информации с целью поддержания возможности ООО «Медицинский центр «Лазер» оказания услуг высокого качества и принятию эффективных управленческих решений;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в ООО «Медицинский центр «Лазер»

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 Генеральному директору.

## 3. ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕГО ПОЛОЖЕНИЯ

Требования настоящего Положения распространяются на всю информацию и ресурсы обработки информации в ООО «Медицинский центр «Лазер». Соблюдение настоящего Положения 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 настоящего Положения.

ООО «Медицинский центр «Лазер» 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, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала.

## 4. КОНТРОЛЬ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

Все работы в пределах офиса ООО «Медицинский центр «Лазер» выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в организации.

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 центра производится только при согласовании с Генеральным 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 КОМПАНИИ

Каждый сотрудник обязан немедленно уведомить Генерального директора обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети. 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 Центра с учетом их взаимоотношений с Центром.

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

Сотрудникам, работающим за пределами Центра с использованием компьютера, не принадлежащего Центру, 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 ООО «Медицинский центр «Лазер».

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 ООО «Медицинский центр «Лазер» 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 ООО «Медицинский центр «Лазер» не должны использовать сеть Интернет для хранения корпоративных данных;
- сотрудники ООО «Медицинский центр «Лазер» при работе с Интернет-ресурсами должны пользоваться только режимом просмотра информации, исключая возможность передачи информации в сеть Интернет;
- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем ООО «Медицинский центр «Лазер»;
- сотрудники ООО «Медицинский центр «Лазер» перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть ООО «Медицинский центр «Лазер» для всех лиц, не являющихся сотрудниками Компании, включая членов семьи сотрудников.
- Руководство ООО «Медицинский центр «Лазер» 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 ООО «Медицинский центр «Лазер», является собственностью центра 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.

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 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.

## 10. ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Все программное обеспечение, установленное на предоставленном ООО «Медицинский центр «Лазер» компьютерном оборудовании, является собственностью центра 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 генеральному директору ООО «Медицинский центр «Лазер».

На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- антивирусное программное обеспечение.
- все компьютеры, подключенные к корпоративной сети, должны быть оснащены системой антивирусной защиты, утвержденной руководителем ООО «Медицинский центр «Лазер».
- Сотрудники Центра не должны:
- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

## 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 ООО «Медицинский центр «Лазер» по электронной почте. Строго конфиденциальная информация ООО «Медицинский центр «Лазер», ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

Сотрудникам ООО «Медицинский центр «Лазер» запрещается использовать публичные почтовые ящики электронной почты для осуществления какого-либо из видов корпоративной деятельности.

Сотрудники ООО «Медицинский центр «Лазер» 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.

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 руководителя ООО «Медицинский центр «Лазер».

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 ООО «Медицинский центр «Лазер» сообщений/писем;
- рассылка рекламных материалов, не связанных с деятельностью Центра;
- 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, злым 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 ООО «Медицинский центр «Лазер» 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 Генеральному директору.

Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник ООО «Медицинский центр «Лазер» обязан:

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

## 13. УПРАВЛЕНИЕ СЕТЬЮ

Уполномоченный сотрудник по информационным технологиям контролируют содержание всех потоков данных, проходящих через сеть Центра.

Сотрудникам Центра 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 сотрудниках или списки сотрудников и пациентов ООО «Медицинский центр «Лазер» посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

## 14. 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 Генеральным 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.

#### 15. РАЗРАБОТКА СИСТЕМ И УПРАВЛЕНИЕ ВНЕСЕНИЕМ ИЗМЕНЕНИЙ

Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть согласованы с Генеральным директором ООО «Медицинский центр «Лазер».