Приложение
к приказу ООО «ДЕНТА»_____№ 4
от «09» января 2017 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ООО «ДЕНТА»

СТАВРОПОЛЬСКИЙ КРАЙ ГОРОД КУРОРТ ЖЕЛЕЗНОВОДСК

Железноводск 2017

1.Общие положении

1.1.Настоящая Политика информационной безопасности (далее - Политика) разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов федерального органа исполнительной власти, уполномоченного в области защиты прав субъектов персональных данных, федерального органа исполнительной власти, уполномоченного в обладет обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

1.2.Настоящая Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности защищаемой в стоматологической клинике ООО «ДЕНТА». Руководство и сотрудники ООО»ДЕНТА» осознают важность развития и совершенствования мер и средств обеспечения информационной безопасности.

1.3.Настоящая Политика является общедоступным документом и представляет собой официально принятую руководством ООО «ДЕНТА» систему взглядов на проблему обеспечения информационной безопасности.

1.4.В Политике определены принципы построения системы обеспечения информационной безопасности, требования к системе обеспечения информационной безопасности, требования к персоналу, степень ответственности персонала, классификация и должностью обязанности персонала, ответственного за обеспечение безопасности защищаемой в ООО «ДЕНТА» информации.

1.5.Целью настоящей Политики является обеспечение безопасности объектов защиты от всех видов актуальных угроз, внешних и внутренних, умышленных и непреднамеренных, а так же минимизация ущерба от реализации угроз информационной безопасности.

1.6.Обеспечение безопасности объектов защиты достигается выполнением требований:

*российского законодательства в области защиты персональных данных и врачебной тайны;

•нормативных актов федерального органа исполнительной власти, уполномоченного в области защиты нрав субъектов персональных данных:

*нормативных актов федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности;

•нормативных актов федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

1.7.Безопасность защищаемой информации достигается путем выявления актуальных угроз безопасности информации и применения мер, направленных па компенсацию актуальных угроз безопасности информации.

1.8.Требования настоящей Политики могут быть детализированы в Положениях о порядке обработки и обеспечении безопасности к конкретным информационным системам, которые разрабатываются как отдельные внутренние нормативные документы, в установленном порядке утверждаются руководством ООО «ДЕНТА» Положения о порядке обработки и обеспечении безопасности к конкретным информационным системам не могут Противоречить положениям настоящей Политики.

2.Область действия

1,Настоящая Политика затрагивает вес виды деятельности ООО «ДЕНТА», касающиеся обработки персональных данных и врачебной тайны,

2.Требования настоящей Политики должны неукоснительно соблюдаться персоналом ООО «ДЕНТА» и лицами, с которыми ООО «ДЕНТА» взаимодействует в силу специфики своей работы или договорных отношений, в соответствии с нормативными документами и договорами, регламентирующими такие отношения.

3.Объекты защиты

3.1.Основными объектами защиты системы обеспечения информационной безопасности являются:

•информационные ресурсы, содержащие врачебную тайну, персональные данные физических лиц, сведения ограниченного распространения , а также открыто

распространяемая информация, необходимая для работы ООО «ДЕНТА». независимо от формы и вида ее представления;

•информационная инфраструктура, включающая системы обработки информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;

•сотрудники ООО «ДЕНТА» прямо иди косвенно связанные с работой информационных систем ООО «ДЕНТА»

3.2.Детализированные перечни подлежащей защите информации утверждаются руководством ООО «ДЕНТА»

4.Угрозы информационной безопасности

4.1.Актуальные угрозы информационной безопасности определяются для каждой информационной системы отдельно на основании частной модели угроз или частной модели нарушителя, которые в установленном порядке утверждаются руководством ООО «ДЕНТА».

4.2.Частные модели угроз или частные модели нарушителя разрабатываются в соответствии с нормативными документами федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

4.3.Для компенсации актуальных угроз, выявленных на основании частной модели угроз и частой модели нарушителя, принимает организационные и технические меры в соответствии с требованиями нормативных документов федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации.

4.4.Перечень организационных и технических мер, направленных на компенсацию актуальных угроз, утверждается руководством ООО «ДЕНТА».

4.5.И соответствие требованиями законодательства Российской Федерации принятые организационные и технические меры подлежат обязательной оценки эффективности, которую ООО «ДЕНТА»» может провести как самостоятельно, так и с привлечением третьих лиц. имеющих лицензию па осуществление деятельности по технической защите конфиденциальной информации. Указанная оценка проводится не реже одного раза в 3 года

5.Система обеспечения информационной безопасности

5.1.Система обеспечения информационной безопасности строится на сбалансированном применении взаимодополняющих организационных и технических мер компенсации угроз информационной безопасности.

5.2.Для эффективного построения и своевременного совершенствования системы обеспечения информационной безопасности используется Цикл Шухарта-Демнига (цикл PDCA) «планирование-действие-корректировка».

5.3.При планировании системы обеспечения информационной безопасности осуществляются:

•определение и распределение прав, обязанностей и ответственности персонала:

•определение и оценка важности информации, подлежащей защите;

•анализ применяемых технологий;

•определение угроз информационной безопасности;

*выбор защитных мер, противодействующих реализации угроз безопасности информации и минимизирующих возможные негативные последствия в случае их реализации:

*оценка влияния защитных мер на деятельность организации;

*оценка затрат на реализацию защитных мер;

рассмотрение и оценка различных вариантов построения системы обеспечения информационной безопасности:

*выбор конкретной реализации системы обеспечения информационной безопасности.

5.4.В рамках реализации действий по построению и совершенствованию системы обеспечении информационной безопасности осуществляются:
*сбор информации о событиях информационной безопасности;
*выявление и анализ инцидентов информационной безопасности;
*расследование инцидентов информационной безопасности:
*оперативное реагирование па инцидент информационной безопасности;
*минимизация негативных последствий инцидентовинформационной безопасности:
*оперативное доведение до руководства информации но наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним:
*выполнение принятых решений по всем инцидентаминформационной безопасности в установленные сроки;
*пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
*повышение уровня знаний персонала в вопросах обеспечения информационной безопасности;
*контроль доступа в здания и помещения;
*обеспечение защиты информации от утечки по техническим каналам;
*применение средств защиты информации;
*обеспечение бесперебойной работы систем и сетей связи;
*обеспечение возобновления работы систем и сетей связи после прерываний и нештатных ситуаций;
*обеспечение информационной безопасности на стадиях жизненного цикла информационных систем (проектирование, разработка, приобретение, поставка, ввод в эксплуатацию, сопровождение);
*обеспечение информационной безопасности при использовании доступа в сети общего доступа.
5.5.В целях реализации проверки системы обеспечения информационной безопасности осуществляются:
*контроль правильности реализации защитных мер;
*контроль системы обеспечения информационной безопасности во время эксплуатации:
*контроль изменений конфигурации системы обеспечения информационной безопасности;
*контроль исполнения персоналом требований внутренних нормативных документов по обеспечению информационной безопасности;
*контроль деятельности пользователей информационных систем, направленный на выявление несанкционированной деятельности.
5.6.В целях совершенствования системы обеспечения информационной безопасности осуществляется периодическое, а при необходимости оперативное, уточнение и/млн пересмотр выбранных мер обеспечения информационной безопасности.
5.7.Для реализации системы обеспечения информационной безопасности руководством ООО «ДЕНТА» назначается ответственное лицо, которое координирует действия подразделения по вопросам информационной безопасности. Ответственное лицо выполняет следующие функции;
*соблюдение действующею законодательства по вопросам информационной безопасности;
*определение необходимых мер обеспечения информационной безопасности;
*разработка внутренних нормативных документов но обеспечению информационной безопасности;
*осуществление контроля актуальности и непротиворечивости внутренних нормативных документов по обеспечен ню и информационной безопасности;
*обучение и контроль персонала по вопросам информационной безопасности;
*планирование и координация внедрения мер обеспечения информационной безопасности;
* выявление и предотвращение угроз информационной безопасности;
*выявление и реагирование па инциденты информационной безопасности;

*мониторинг и оценка эффективности принятых мер обеспечения информационной безопасности,
*информирование руководства и руководителей структурных подразделении об угрозах информационной безопасности.
5.8.Исхода из требований действующего законодательства, результатов проведения внутренней проверки, перечня информации, подлежащих защите определяется необходимый уровень защищенности информационных систем. На основании анализа актуальных угроз безопасности защищаемой информации, описанных в частной модели угроз, выполняется заключение о необходимости использования конкретных технических и организационных мер обеспечения безопасности защищаемой информации. Необходимые мероприятия отражаются в плане мероприятии по обеспечению безопасности защищаемой информации.
5.9. Организационные меры обеспечения безопасности защищаемой информации заключается в установлении
режима ограниченного доступа к защищаемом информации. Состав организационных мер включает;
* утверждение списка лиц, допущенных к работе с защищаемой информацией;
* утверждение прав, обязанностей и ответственности лиц, допущенных к работе защищаемой информацией;
* утверждение списка помещений, в которых разрешено обрабатывать защищаемую информацию;
* утверждение прав разграничения доступа к защищаемой информации;
* утверждение контролируемой зоны;
*утверждение нормативных документов регламентирующих правила обработки защищаемой информации;
* планирование мероприятий по защите информации,
5.10.В зависимости от класса информационной системы и актуальных угроз, технические меры обеспечения информационной безопасности могут включать в себя следующие подсистемы;
*идентификации и аутентификации субъектов доступа и объектов доступа;
*управления доступом субъектов доступа к объектам доступа;
*ограничения программной среды;
*зашиты машинных носителей информации;
*регистрации событий безопасности;
*антивирусной защиты;
*обнаружения вторжений;
*контроля и анализа защищенности;
*обеспечения целостности;
*обеспечения доступности;
*защиты среды виртуализации;
*защиты технических средств;
*защита информационной системы, ее средств, систем связи и передачи данных;
*выявления инцидентов информационной безопасности;
*управления конфигурацией информационной системы и системы защиты;
*криптографической защиты,
5.11.Требования к подсистемам системы обеспечения информационной безопасности устанавливаю к-я нормативными актами федерального органа исполнительной власти, уполномочен ною в области обеспечения безопасности и федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации,
5.12.Список конкретных используемых технических средств фиксируется документально и должен поддерживаться в актуальном состоянии, При изменении состава технических средств защиты или элементов информационных систем, соответствующие изменения должны быть внесены и утверждены руководством ООО «ДЕНТА».

6.Классификация персонала, участвующего в обработке защищаемой информации

6.1.В зависимости от выполняемых должностных обязанностей можно выделить следующие группы персонала, участвующих в обработке защищаемой информации:

*разработчики информационных систем

*администраторы информационных систем;

*администратора безопасности информационных систем;

*операторы информационных систем;

*специалисты сервисного обслуживания оборудования информационных систем.

6.2.Администраторы информационных систем сотрудники, ответственные за настройку, внедрение и сопровождение информационных систем. Обеспечивают функционирование подсистемы управления доступом и уполномочены осуществлять предоставление и разграничение доступа конечного пользователя (оператора) к элементам, обрабатывающим защищаемую информацию. Администраторы обладают следующим уровнем доступа и знаний:

*обладает полной информацией о системном и прикладном программном обеспечении информационных систем;

*обладает полной информацией о технических средствах и конфигурации информационных систем;

* имеет доступ ко всем техническим средствам обработки информации и данным информационных систем;

* обладает правами конфигурирования и административной настройки технических средств информационных систем, Администраторы безопасности - сотрудники, ответственные за функционирование системы защиты информации. Администраторы безопасности обладает следующим уровнем доступа и знаний;

*обладает правами Администратора в объеме необходимо для выполнения своих сложных обязанностей;

*обладает полной информацией об информационных системах;

* имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационных систем;

*нс имеет прав доступа к конфигурированию технических средств за исключением контрольных инспекционных).администраторы безопасности уполномочены:

* реализовывать политики безопасности в части настройки подсистем системы защиты информации;

*осуществлять аудит системы защиты информации;

*устанавливать доверительные отношения между информационными системами.

6.3.Опера горы информационных систем - сотрудники, осуществляющие обработку защищаемой информации. Оператор не имеет полномочий для управления подсистемами информационных систем и системы защиты информации.

Операторы обладают следующим уровнем доступа и знаний:

*обладает всеми необходимыми атрибутами, обеспечивающими доступ к некоторому подмножеству защищаемой информации;

*располагает' защищаемой информацией, к которой имеет доступ.

6.4.Специалисты сервисного обслуживания оборудования информационных систем сотрудники, осуществляющие обслуживание и настройку оборудования информационных систем. Технический специалист по обслуживанию не имеет доступа к защищаемой информации, не имеет полномочий для управления подсистемами информационных систем и системы защиты информации.

Специалисты сервисного обслуживания оборудования информационных систем обладают следующим уровнем доступа и знаний:

*обладает частью информации о системном и прикладном программном обеспечении информационных систем:

*обладает частью информации о технических средствах и конфигурации информационных систем;

6.5.Разработчики информационных систем поставщики прикладного программного

обеспечения, обеспечивающие его сопровождение на защищаемом объекте, могут быть как штатными сотрудниками, так и представителями сторонних организаций.
Разработчики информационных систем обладают следующим уровнем доступа и знаний:
*обладает информацией об алгоритмах и программной реализации обработки информации в информационных системах;
*обладает возможностями внесения ошибок, не декларированных возможностей, программных закладок, вредоносных программ в программное обеспечение информационных систем на стадии ее разработки, внедрения и сопровождения;
*может располагать любыми фрагментами информации о топологии и технических средствах обработки и защиты информации, обрабатываемых в информационных системах.
Разработчики информационных систем работают на договорной основе, поэтому в договор должен быть внесем пункт об обеспечении безопасности информации в разрабатываемых информационных системах, об ответственности разработчики в случаи обнаружения не декларируемых возможностей в разработанной информационной систем или в случаи возникновения инцидента информационной безопасности, возникшего по вине разработчика информационной системы.

7.Требовании к персоналу

7.1. Все сотрудники, имеющие право доступа к защищаемой информации, должны четко знать и строго выполнять установленные правила доступа к защищаемой информации и соблюдению принятого режима безопасности защищаемой информации.
7.2.При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает', обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования но защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем.
7.3.Сотрудник должен быть ознакомлен о требованиями действующего законодательства, настоящей Полит ики и утвержденных локальных нормативных актов.
7.4.Сотрудники должны следовать установленным процедурам поддержании режима безопасности информации.
7.5.Сотрудники должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.
7.6.Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
7.7.Сотрудникам запрещается разглашать третьим лицам защищаемую информацию.
7.8.При работе с защищаемой информацией сотрудники обязаны обеспечить отсутствие возможности просмотра защищаемой информации третьими лицами.
7.9.При завершении работы с информационными системами сотрудники обязаны ограничить доступ к информационным системам с помощью блокировки или эквивалентного средства контроля.
7.10.Сотрудники должны быт проинформированы об угрозах нарушения режима безопасности защищаемой информации и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности защищаемой информации.
7.11.Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационных систем, способных повлечь за собой реализацию угрозы безопасности защищаемой информации, а также о выявленных ими инцидентах информационной безопасности руководству подразделения и ответственному лицу.

8.Ответственность за соблюдение положений Политики

Ответственность персонала за невыполнение настоящей Политики определяется в соответствующих пунктах, включаемых в трудовые договоры и/или должностные

инструкции, а также положениями внутренних нормативных документов.

9.Заключительные положения

9.1.Требования настоящей Политики могут развиваться другим внутренними нормативными документами, которые дополняют и уточняют ее.

9.2.В случае изменения действующего законодательства и иных нормативных актов настоящая Политика и изменения к пей применяются в части, нс противоречащей вновь принятым законодательным и иным нормативным актам.

9.3.Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

*периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 3 года;

*внеплановое внесение изменений в настоящую Политику может производиться но результатам анализа защищенности информационных систем или изменении действующего законодательств и локальных нормативных актов,

9.4.Ответственным за внесение изменении в настоящую Политику является лицо ответственное за организацию работ по обеспечению информационной безопасности.