Утверждена
приказом директора больницы
от «29» декабря 2023 года №163-о

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ

Содержание

Общие положения.
Основные задачи Политики
Ссылки на документы
Область применения.
Право собственности.
Изложение содержания Политики
Детальные политики в информационной безопасности области.
Обеспечение соблюдения политики информационной безопасности и принятие мер в случае ее нарушения.
Приложения
Приложение А. «Паспорт рабочей станции пользователя».
Приложение Б. «Журнал заявок пользователей».
Приложение В «Журнал измерения температуры и влажность серверной комнаты».
Приложение Г. «Журнал посещение серверной комнаты».
Приложение Д «Журнал внештатных ситуаций».
Приложение Е «Регламент действия персонала во внештатных ситуациях».
Приложение Ж. «Техника безопасности при работе с персональным компьютером».
Приложение З. «Журнал доступа сотрудников Больницы к информационным системам МЗ РК».
Приложение И. «Правило резервного копирования, хранения резервных файлов и восстановления в случае чрезвычайных ситуаций».
Приложение К. План обучения медицинских работников.
по ИС МЗ РК.
Приложение Л «Заявка на проведение обучения персонала».
Приложение М «Защита информации».
Приложение Н «Инструкция по обеспечению парольной защиты».
Приложение О «Регламент по проведению системно-технического обслуживания программно-аппаратных средств, информационных систем»

Приложение П «Лист согласования».

Приложение Р «Лист ознакомления».

Приложение С «Лист регистрации изменений»

1 Общие положения

1.1 Политика информационной безопасности (далее- Политика) устанавливает степень ответственности и обязанности по обеспечению информационной безопасности ГКП на ПХВ «Многопрофильная городская детская больница №2» акимата города Астаны (далее –Больница), определяет направления разработки соответствующих процедур и мер контроля, внедрение которых послужит достижению ее реализации.

2 Основные задачи Политики

2.1 Обеспечение непрерывности доступа к информационным ресурсам Больницы с целью осуществления деятельности в соответствии с действующим законодательством.

2.2 Защита целостности деловой информации с целью поддержания возможности Больницы по оказанию медицинских услуг высокого качества и принятию эффективных управленческих решений.

2.3 Сохранение конфиденциальности критичных информационных ресурсов.

2.4 Построение четкой системы учета информационных ресурсов Больницы с целью их эффективного использования и управления.

2.5 Обеспечение внедрения обоснованных, экономически эффективных и последовательных мер контроля и процедур в области информационной безопасности во всех подразделениях и информационно- технологических системах и сетях Больницы.

2.6 Повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Больницы.

2.7 Обеспечение возможности применения Больницей установленных санкций и защита законных прав сотрудников в соответствии с действующим законодательством в случае неправильного или неправомерного использования информационных ресурсов Больницы.

3 Ссылки на документы

МС ИСО 9000:2005	Системы менеджмента качества. Основные положения и словарь
СТ РК ИСО 9000-2007	Системы менеджмента качества. Основные положения и словарь
МС ИСО 9001:2008	Системы менеджмента качества. Требования
СТ РК ИСО 9001-2009	Системы менеджмента качества. Требования
СТ РК 989-2008	«Организационно-распорядительная документация требования к оформлению документов».
Закон Республики Казахстан N 217 – III от 11.01.2007г.	«Об информатизации»
Постановление правительства Республики Казахстан №1605 от 26 декабря 2011 года.	«Перечень типовых документов, образующихся в деятельности государственных и негосударственных организаций, с указанием сроков хранения».
Постановление правительства Республики Казахстан №1153 от 22 декабря 2011 года.	«Правила приема, хранения, учета и использования документов Национального архивного фонда и других архивных документов ведомственными и частными архивами».
Постановление правительства Республики Казахстан №1604 от 26 декабря 2011 года	«Правила комплектования, хранения, учета и использования документов Национального архивного фонда, других архивных документов государственными и специальными государственными архивами»
Постановление правительства Республики Казахстан №1705 от 21 декабря 2011 года.	«Типовые правила документирования и правления документацией в государственных и негосударственных организациях».

4 Область применения

4.1 Требования настоящей Политики распространяются на всю информацию и ресурсы по обработке данных Больницы.

4.2 Соблюдение Политики обязательно для всех: для руководства,сотрудников (как постоянных, так и временных), а также третьих лиц, имеющих доступ к информационным ресурсам Больницы.

5 Право собственности

5.1 Больницепринадлежит по праву собственности вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством.

5.2 Указанное правособственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Больницы, лицензионное и разработанное программное обеспечение, внутренние и внешние сообщения электронной почты и прочее содержаниеящиков электронной почты, бумажные и электронные документы всех функциональных отделов и персонала Больницы.

6 Изложение содержания Политики

6.1 Ресурсы компьютерных систем и соответствующая корпоративная информация представляют собой важные активы, требующие высокого уровня защиты.

6.2 Политика Больницыпредусматривает принятие необходимых мер в целях защиты таких активов от случайного или несанкционированного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности и целостности информации и обеспечения процесса автоматизированной обработки данных в Больницы.

6.3 Обеспечение информационной безопасности является обязанностью всех сотрудников Больницы, при этом обеспечение безопасности всех активов Больницы является задачей первоочередной важности.

7 Детальные политики в информационнойбезопасности области

7.1 В дополнение к общей Политике разработан набор документов в области информационной безопасности.

7.2 В комплект нормативных документов в области информационной безопасности включены следующие документы:

Название детальной политики	Периодичность действия	Ответственные	
		Все	Программист
Паспорт рабочих станции пользователей(приложение А).	Всегда		+
Журнал заявок пользователей (приложение Б).	Ежедневно		+
Журнал измерения температуры и влажности серверной комнаты(приложение В).	Ежедневно		+
Журнал посещения серверной комнаты (приложения Г).	Всегда	+	
Журнал регистрации внештатных ситуаций	Всегда	+	

(приложения Д).			
Регламент действия персонала во внештатных ситуациях(приложения Е).	Всегда	+	
Техника безопасности при работе с персональным компьютером (приложения Ж).	Всегда	+	
Журнал доступа сотрудников Больницы к информационным системам (приложения З).	Всегда	+	
	Всегда	+	
Правила резервного копирования, хранения резервных файлов и восстановления в случае чрезвычайных ситуаций (приложения И).	Ежедневно		+
План обучения медицинских работников Больницы по ИС (приложение К)	Ежегодно		+
Заявка на проведение обучения Персонала (приложение Л)	Ежемесячно		+
Защита информации (приложение М)	Всегда	+	
Инструкция по обеспечению парольной защиты (приложение Н)	Всегда	+	
Регламент по проведению системно-технического обслуживания программно-аппаратных средств, информационных систем (приложение О)	Ежеквартально		+

7.3 Указанные документы хранятся у программиста Больницы. Соответствующие документы дорабатываются и обновляются программистомна постоянной основе с целью поддержания их в актуальном состоянии.

8 Обеспечение соблюдения Политики и принятие мер в случае нарушения

8.1 Руководители подразделений Больницы должны обеспечить регулярный контроль за соблюдением настоящей Политики в соответствии с установленными стандартами и процедурами контроля, определенных в рамках комплекта нормативных документов в области информационной безопасности. Кроме того, должна быть организована периодическая проверка соблюденияинформационной безопасности.

8.2 Случаи несоблюдения настоящей Политики подлежат подробному расследованию и должны разрешаться в соответствии с действующим законодательством и могут привести к принятию дисциплинарных мер взыскания к виновным вплоть до увольнения.

8.3 Любые преднамеренные действия, предпринимаемые с целью нарушить, блокировать или иным способом обойти установленные средства контроля в области информационной безопасности, а также блокировать или противодействовать работе технических средств по регистрации или

8.3 Любые преднамеренные действия, предпринимаемые с целью нарушить, блокировать или иным способом обойти установленные средства контроля в области информационной безопасности, а также блокировать или противодействовать работе технических средств по регистрации или направлению сообщений о нарушениях в системе защиты, рассматриваются как потеря доверия и могут привести к немедленному увольнению виновного.

8.4 Больница оставляет за собой право на просмотр любой информации, которая хранится, передается или обрабатывается в ее компьютерных или телекоммуникационных системах и на соответствующих носителях данных, контролировать использование вычислительных ресурсов с точки зрения производственной необходимости, а также отказывать в предоставлении доступа или аннулировать доступ любого лица или принимать дисциплинарные меры взыскания к любому лицу с целью обеспечения соблюдения настоящей политики.

Разработано:
Начальником отдела _____ **Ж. Кыстаубаев**