Код			
Название	**Политика информационной безопасности**		
Дата разработки	4 января 2018 года		
Дата утверждения	Приказом Главного врача ГКП на ПХВ «Перинатального центра №3» акимата города Астаны № от «8» января 2018 года		
Дата следующего пересмотра	8 января 2020 г.		
Разработчик	Должность	ФИО	подпись
		Кусаинов Т.Г.	
Согласовано	Главный врач	Хамидуллина З.Г.	
	Служба поддержки пациентов и внутреннего аудита	Досмырзаева Г.Т.	
	Главная медицинская сестра	Садвакасова М.А.	
Версия №			

1. Цель обеспечения информационной безопасности

Политика информационной безопасности ГКП на ПХВ «Перинатальный центр №3» акимата города Астаны (далее – ПЦ№3) определяет цели и задачи системы обеспечения информационной безопасности (ИБ) и устанавливает совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется ПЦ №3 в своей деятельности.

Основной целью ПЦ№3 является обеспечение информационной безопасности, что предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности, подчиненное единому замыслу.

Общее руководство обеспечением ИБ осуществляет Главный врач ПЦ№3. Ответственность за организацию мероприятий по обеспечению ИБ и контроль за соблюдением требований Начальник службы поддержки пациентов и внутреннего аудита.

Руководители структурных подразделений ПЦ№3 ответственны за обеспечение выполнения требований ИБ в своих подразделениях.

Сотрудники ПЦ№3 обязаны соблюдать порядок обращения с конфиденциальной медицинской документацией, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов ИБ.

2. Нормативные ссылки

2.1 Закон Республики Казахстан от 23 января 2001 года №148 «О местном государственном управлении и самоуправлении в РК» (измененииями и дополнениями по состоянию на 09.02.2009г.)
2.2 Закон Республики Казахстан 11 января 2007 года № 217 – 3 об информатизации.
2.3 Закон Республики Казахстан от 15 марта 1999 года №349-1 «О государственных секретах»
2.4Указ Президента Республики Казахстан от 10 октября 2006 года № 199 «О концепции информационной безопасности РК»

3. Термины и определения

АС – Автоматизированная система.
БД – База данных.
ЗИ – Защита информации.
ИБ – Информационная безопасность.
ИС – Информационная система.
БГ – Бюро госпитализации
ЕИСЗ – Единые информационные системы здравоохранения
ОС – Операционная система
РБЖиФВ – Регистр беременных и женщин фертильного возраста
АИС поликлиника – Автоматизированная информационная система
ЭРСБ – Электронный регистр стационарных больных
РПН – Регистр прикрепленного населения
СУР – Система управления ресурсами

Доступ к информации – возможность получения информации и ее использования.

Информационная безопасность – механизм защиты, обеспечивающий конфиденциальность, целостность, доступность информации; состояние защищенности информационных ресурсов ПЦ №3 в условиях угроз в информационной сфере. Угрозы могут быть вызваны непреднамеренными ошибками персонала, неправильным функционированием технических средств, стихийными бедствиями или авариями (пожар, наводнение, отключение электроснабжения, нарушение телекоммуникационных каналов и т.п.), либо преднамеренными злоумышленными действиями, приводящими к нарушению информационных активов ПЦ №3.

Информационная система – совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения задач подразделений ПЦ №3. В ПЦ №3 используются различные типы информационных систем для решения управленческих, учетных, обучающих и других задач.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Республики Казахстан.

Конфиденциальность – доступ к информации только авторизованных пользователей.

Локальная вычислительная сеть (ЛВС) – группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

4. Ответственность

Организация просвещения сотрудников ПЦ№3 в области информационной безопасности возлагается на главного врача. Обучение сотрудников ПЦ№3 правилам обращения с конфиденциальной информацией, проводится путем:

-проведения инструктивных занятий с сотрудниками, принимаемыми на работу в ПЦ№3;

-самостоятельного изучения сотрудниками внутренних нормативных документов ПЦ№3.

Допуск персонала к работе с защищаемыми информационными ресурсами ПЦ№3 осуществляется только после его ознакомления с настоящими политиками, а также иными инструкциями пользователей отдельных информационных систем.

5. Доступ к информации и меры безопасности

5.1 Конфиденциальность информации обеспечивается в соответствии с уставными нормами.

5. 2 Обмен, раскрытие кодов доступа, паролей строго запрещен, доступ каждого пользователя ограничен информацией/функциями его полномочий.

5.3 Доступ к компьютерной информации/медицинской документации контролируется уровнем доступа.

5.4 Уровни доступа:

1) Медицинский персонал имеет доступ к программным комплексам ЭРСБ, РПН, РБЖиФВ, АИС поликлиника, БГ, КМИС, СУР, СУКМУ.

2) Сотрудники финансово-экономического отдела имеют доступ к программам 1С, ЭРСБ (счет-реестров)

3) Базовый уровень доступа имеет технический, средний медицинский персонал через установленные учетные записи на компьютерах «Гость».

5.5 Категории сотрудников ПЦ№3, которые обязаны сохранять ИБ и целостность данных, имеющих доступ к медицинской документации:

1) Инженерная группа по IT-поддержке;

2) руководители клинико-диагностической лаборатории;

3)персонал структурного подразделения;

4)сотрудники статистических отделов стационара и женской консультации.

5.6. Доступ по локальной сети: чтение и изменение.

6. Доступ к сети Интернет

6.1 Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

6.2 Рекомендованные правила:

· сотрудникам ПЦ№3 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 ПЦ№3 перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

7. Защита оборудования

7.1 Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация ПЦ №3.

8. Программное обеспечение

8.1 Все программное обеспечение, установленное на предоставленном ПЦ компьютерном оборудовании, является собственностью ПЦ№3 и должно использоваться исключительно в производственных целях.

8.2 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 главному врачу.

9. Профилактика нарушений политик информационной безопасности

9.1 Под профилактикой нарушений политик информационной безопасности понимается проведение регламентных работ по защите информации, предупреждение возможных нарушений информационной безопасности в ПЦ№3 и проведение разъяснительной работы по информационной безопасности среди пользователей.

9.2 Прием на работу новых сотрудников должен сопровождаться ознакомлением их с правилами и требованиями настоящих политик.