УТВЕРЖДЕНА
приказом № 24
от «04» 01 2018 года

ПОЛИТИКА
информационной безопасности
ГКП на ПХВ «Городская поликлиника №17»
Управления здравоохранения города Алматы

Согласовано:

	Должность	ФИО	Подпись
1.	Заместитель главного врача по лечебной работе	Достоярова Б.О.	
2.	Заведующая статистическим кабинетом	Калиева К.С.	
3.	Эксперт	Мекебекова А.О.	
4.	Инспектор отдела кадров	Абдибаева А.Е.	
5.	Юрист	Филимонова Н.В.	

Разработано:

	Должность	ФИО	Подпись
1.	Программист	Абдигапбарулы А.	

1. Общие положения и цели

1.1. ГКП на ПХВ "Городская поликлиника №17" Управления здравоохранения города Алматы (далее ГП № 17) является предприятием, осуществляющим деятельность в области здравоохранения путем оказания амбулаторно-поликлинической помощи прикрепленному населению.

1.2. Политика информационной безопасности ГКП №17 устанавливает цели, задачи и подходы в области информационной безопасности, которыми ГКП № 17 руководствуется в своей деятельности.

1.3. Политика направлена на достижение следующих целей: _ обеспечение непрерывности основных бизнес-процессов ГКП № 17 ; _ минимизация

возможных потерь и ущерба от нарушений в области информационной безопасности.

2. Управление информационной безопасностью

2.1. Для достижения указанных целей в ГКП №17 внедряется система управления информационной безопасностью (далее — СУИБ), которая соответствует:

-Постановлению Правительства Республики Казахстан от 20 декабря 2016 года N 832 «Об утверждении Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»

-требованиям законодательства Республики Казахстан, нормативным и договорным обязательствам ГКП №17 по информационной безопасности.

2.2. СУИБ документирована в настоящей Политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников ГКП №17 в области действия системы. Документированные требования СУИБ доводятся до сведения работников ГКП №17.

2.3. Все информационные активы ГКП №17, включая аппаратное обеспечение, программное обеспечение, информационные ресурсы на бумажных и электронных носителях, подлежат учету и категорированию в соответствии с их важностью и степенью доступа.

2.4.В соответствии с установленными процедурами в области управления рисками, осуществляется регулярная оценка рисков информационной безопасности. При ее проведении учитывается вероятность угроз информационной безопасности и степень их влияния на бизнес— процессы, финансовое состояние и деловую репутацию ГКП №17.

2.5. По результатам оценки рисков информационной безопасности выбираются и применяются средства управления для защиты информации, включая организационные, физические, технические, программные и программно—аппаратные средства обеспечения СУИБ.

2.6. ГКП №17 стремится выявлять, учитывать и реагировать на инциденты в сфере информационной безопасности в соответствии с установленными процедурами.

2.7. В ГКП №17 будут установлены процедуры обеспечения непрерывности критических бизнес—процессов от эффектов существенных сбоев информационных систем или чрезвычайных ситуаций, контроля работоспособности СУИБ.

2.8. Работники ГКП №17 получают доступ к той информации, которая требуется для исполнения их функциональных обязанностей. ГКП №17 проводит информирование, обучение и повышение квалификации

работников, чья деятельность связана с информационной системой здравоохранения в сфере информационной безопасности.

2.9. ГКП №17 производит пересмотр Политики информационной безопасности ГКП №17 (далее Политика) в соответствии с изменениями, влияющими на первоначальную оценку риска, путем выявления существенных инцидентов нарушения информационной безопасности, появления уязвимостей или изменения организационной или технологической инфраструктуры.

3. Ответственность

3.1. Руководство ГКП №17 осуществляет общее управление информационной безопасностью ГКП №17 и обеспечивает необходимые условия для:

- реализации мероприятий по оценке рисков информационной безопасности и защиты информации;
- поддержания, проведения мониторинга, анализа и непрерывного улучшения системы управления информационной безопасностью;
- регулярного обучения работников по вопросам в сфере информационной безопасности в соответствии с утвержденным графиком (сроки, тематика, периодичность).

3.2. Работники ГКП №17 несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности заместителю первого руководителя, курирующего вопросы по СУИБ.

3.3. В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной документации и конфиденциальность информации, ставшей известной в силу выполнения своих обязанностей.

4. Заключительные положения

4.1. Руководство ГКП №17 заявляет своё одобрение настоящей Политики, которая объявлена, распространена, внедрена и поддерживается на всех уровнях ГКП №17.

4.2. Политика информационной безопасности ГКП №17 является общедоступным документом, который может предоставляться всем заинтересованным сторонам и размещается на официальном веб-сайте ГКП №17.