«ИННОВАЦИЯЛЫҚ ТЕХНОЛОГИЯЛАР МЕН ЗЕРТТЕУЛЕР ҒЫЛЫМИ ОРТАЛЫҒЫ» ЖШС

ТОО «НАУЧНЫЙ ЦЕНТР ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ И ИССЛЕДОВАНИЙ»

УТВЕРЖДЕНО
на заседании
Ученого совета
№1 от 15 января 2025г.

ПРАВИЛА
соблюдения конфиденциальности
и обеспечении целостности служебной информации
ТОО «Научный центр инновационных технологий и исследований»

1. Общие положения
1.1. Настоящие Правила определяют единые требования, принципы и меры по обеспечению конфиденциальности, сохранности и целостности служебной информации в ТОО «Научный центр инновационных технологий и исследований» (далее - Центр).
1.2. Правила являются обязательными для исполнения всеми работниками, привлечёнными экспертами, консультантами, преподавателями, научными сотрудниками, медицинскими работниками, а также иными лицами, получившими доступ к служебной информации Центра.
1.3. Правила разработаны в соответствии с законодательством Республики Казахстан, в том числе в области:
- защиты персональных данных;
- охраны врачебной тайны;
- коммерческой и служебной тайны;
- интеллектуальной собственности;
- обеспечения информационной безопасности.

1.4. Целью настоящих Правил является:
- защита служебной, медицинской, экспертной, научной и иной информации от несанкционированного доступа, утраты, искажения или разглашения;
- обеспечение доверия со стороны пациентов, заказчиков, партнеров и государственных органов;
- соблюдение принципов профессиональной этики и добросовестности.

2. Основные термины и определения
В настоящих Правилах используются следующие термины:
- **Служебная информация** — любые сведения, создаваемые, используемые или хранимые в Центре в процессе его деятельности, не подлежащие свободному распространению.

- **Конфиденциальная информация** — информация, доступ к которой ограничен в соответствии с законодательством РК и внутренними актами Центра.
- **Целостность информации** — состояние информации, при котором обеспечивается её полнота, достоверность и защита от несанкционированных изменений.
- **Несанкционированный доступ** — получение, использование, изменение или распространение информации без соответствующих полномочий.
- **Субъект доступа** — сотрудник или иное лицо, допущенное к работе с информацией в рамках служебных обязанностей.

3. Виды конфиденциальной информации ТОО «НЦИТИ»

К конфиденциальной информации Центра относятся:

3.1. **Медицинская информация**:
- персональные данные пациентов;
- медицинская документация;
- сведения о диагнозах, лечении, результатах обследований;
- данные клинических исследований и апробаций методик.

3.2. **Экспертная информация**:
- материалы независимой экспертизы качества медицинской помощи;
- экспертные заключения, отчеты, аналитические справки;
- данные аудитов, аккредитационных оценок, проверок.

3.3. **Научная и образовательная информация**:
- результаты НИР, НТП, научные отчеты;
- неопубликованные статьи, методики, учебные материалы;
- авторские разработки, программы обучения, тестовые материалы.

3.4. **Коммерческая и служебная информация**:
- договоры, финансовые расчеты, сметы;
- информация о партнерах и заказчиках;
- стратегии развития, планы, KPI, внутренние отчеты.

3.5. **Информация ограниченного доступа**:
- данные информационных систем;
- логины, пароли, ключи доступа;
- внутренние регламенты и служебная переписка.

4. Принципы обеспечения конфиденциальности и целостности информации

В Центре обеспечивается соблюдение следующих принципов:

4.1. **Законность** — обработка информации осуществляется строго в рамках законодательства РК.

4.2. **Ограничение доступа** — доступ предоставляется только в пределах служебной необходимости.
4.3. **Ответственность** — каждый сотрудник несет персональную ответственность за сохранность информации.
4.4. **Минимизация** — используется только объем информации, необходимый для выполнения конкретных задач.
4.5. **Целостность** — принимаются меры по защите информации от искажения, уничтожения и несанкционированных изменений.
4.6. **Непрерывность защиты** — меры безопасности применяются на всех этапах жизненного цикла информации.

5. Права и обязанности сотрудников
5.1. Сотрудники имеют право:
- получать доступ к служебной информации в пределах своих должностных обязанностей;
- использовать информацию исключительно для служебных целей;
- запрашивать разъяснения по вопросам режима конфиденциальности.

5.2. Сотрудники обязаны:
- соблюдать требования настоящих Правил;
- не допускать разглашения конфиденциальной информации третьим лицам;
- обеспечивать сохранность документов и носителей информации;
- незамедлительно сообщать руководству о фактах утраты, утечки или угрозы безопасности информации;
- подписывать обязательство о неразглашении конфиденциальной информации при приеме на работу или привлечении к проектам.

6. Меры по обеспечению информационной безопасности
6.1. **Организационные меры**:
- разграничение прав доступа;
- ведение учета носителей информации;
- обучение сотрудников вопросам информационной безопасности.

6.2. **Технические меры**:
- использование защищённых информационных систем;
- резервное копирование данных;
- антивирусная защита и контроль доступа.

6.3. **Документальные меры**:
- маркировка документов;
- хранение в защищённых местах;
- регламентированный порядок уничтожения информации.

7. Передача и использование информации

7.1. Передача конфиденциальной информации допускается:

- по официальным каналам связи;
- на основании договоров, соглашений и служебной необходимости;
- с соблюдением требований защиты персональных данных.

7.2. Запрещается:

- использование информации в личных целях;
- копирование и передача без разрешения;
- публикация без согласования с руководством Центра.

8. Ответственность за нарушение конфиденциальности

8.1. Лица, допустившие нарушение требований настоящих Правил, несут ответственность в соответствии с:

- трудовым законодательством РК;
- гражданским и административным законодательством;
- условиями договоров и внутренних актов Центра.

8.2. Нарушения могут повлечь:

- дисциплинарные взыскания;
- материальную ответственность;
- расторжение трудового или гражданско-правового договора.

9. Заключительные положения

9.1. Настоящее Правила вступает в силу с момента утверждения Ученым Советом Центра.

9.2. Все изменения и дополнения в Правила утверждаются приказом руководителя Центра после утверждения вносимых изменений и дополнений Ученым Советом Центра.

9.3. Контроль за исполнением Правил возлагается на руководство Центра и уполномоченных лиц по обеспечению информационной безопасности.