Утверждена
Решением Правления
от 3 марта 2025 года
Протокол № 4

Политика информационной безопасности НАО «Казахский национальный медицинский университет имени С.Д.Асфендиярова»

Срок действия с «3» 03 2025г. по «3» 03 2028г.	Срок продления до «__» _____ 20__ г.	Статус: Действующий □ Устаревший □
Предыдущий устаревший документ: Приказ ректора от №	Подпись ответственного лица за управление документом	Код № 245/7-2025 Копия № Экземпляр №

Алматы – 2025 г.

Лист согласования и подписания

ФИО	Тип действия	Время и дата согласования или подписания	Замечания	Данные по ЭЦП
Сұлтанбай Жансая Мұңайтпасқызы	Разработано	12.03.2025, 12:46:16	Без замечаний	
Альчимбаев Арман Булатович	Согласовано	13.03.2025, 15:14:27	Без замечаний	
Жангирбаев Марат Турсынханович	Согласовано	13.03.2025, 14:21:36	Без замечаний	
Калматаева Жанна Амантаевна	Согласовано	13.03.2025, 14:21:08	Без замечаний	
Султангазиева Светлана Елеусизовна	Согласовано	12.03.2025, 14:36:11	Без замечаний	
Фахрадиев Ильдар Рафисович	Согласовано	12.03.2025, 12:55:49	Без замечаний	
Султангазиева С.Е. (и.о Кайдарова Д.Р.)	Согласовано	13.03.2025, 16:44:02	Без замечаний	
Искаков Серикжан Сагимжанович	Согласовано	13.03.2025, 17:05:59	Без замечаний	
Лахов Сергей Владимирович	Согласовано	12.03.2025, 13:42:33	Без замечаний	
Ахмет Абай Нұржанұлы	Согласовано	13.03.2025, 14:16:49	Без замечаний	
Нагасбекова Баян Серикковна	Согласовано	12.03.2025, 13:16:18	Без замечаний	
Калматаева Ж.А. (и.о Датхаев У.М.)	Подписано	13.03.2025, 17:45:31	Без замечаний	Издатель ЭЦП - ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022, КАЛМАТАЕВА ЖАННА, Некоммерческое акционерное общество "Казахский национальный медицинский университет имени С. Д. Асфендиярова", BIN181240006407
Датхаев Убайдилла Махамбетович	Зарегистрировано	13.03.2025, 17:45:40	Без замечаний	Издатель ЭЦП - ҰЛТТЫҚ КУӘЛАНДЫРУШЫ ОРТАЛЫҚ (GOST) 2022, КАЛМАТАЕВА ЖАННА, Некоммерческое акционерное общество "Казахский национальный медицинский университет имени С. Д. Асфендиярова", BIN181240006407

1. Общие положения

1.1. Настоящая Политика информационной безопасности НАО «Казахский национальный медицинский университет имени С.Д.Асфендиярова» (далее - Политика) разработана в соответствии с действующим законодательством Республики Казахстан, нормативными актами и другими внутренними положениями НАО «Казахский национальный медицинский университет имени С.Д.Асфендиярова» (далее по тексту Университет).

1.2. Настоящая Политика устанавливает правила и требования по обеспечению информационной безопасности в Университете с целью защиты всех информационных ресурсов, включая данные, информационные системы, сети и процессы, от внешних и внутренних угроз.

1.3. Обеспечение информационной безопасности включает в себя защиту информации, систем и сетевой инфраструктуры Университета от несанкционированного доступа, утечек данных, потерь, и иных угроз, способных повлиять на учебный процесс, научную деятельность и репутацию учебного заведения.

1.4. Политика Университета распространяется на все программное и аппаратное обеспечение, а также на информационные ресурсы Университета, включая базы данных, системы хранения, сети, устройства, носители информации и коммуникационные каналы. Она охватывает все уровни взаимодействия с информационными ресурсами: от административных сотрудников и преподавателей до студентов и сторонних организаций, взаимодействующих с Университетом.

1.5. Настоящая Политика должна быть доведена до сведения каждого сотрудника Университета в день заключения трудового договора.

2. Цели и задачи информационной безопасности

2.1 Цели

2.1.1. Основной целью информационной безопасности Университета является обеспечение защиты информации, используемой в учебном процессе и научной деятельности, а также поддержание работоспособности информационных систем и сервисов Университета.

2.1.2. Основные цели информационной безопасности:

1) обеспечение конфиденциальности, целостности и доступности информации;

2) реализация защиты всех информационных ресурсов от несанкционированного доступа и повреждений;

3) предотвращение утечек и потерь информации;

4) обучение сотрудников и студентов основам информационной безопасности;

5) обеспечение своевременного реагирования на инциденты информационной безопасности;

6) обеспечение соответствия внутренним и внешним требованиям по защите информации.

2.1. Задачи

1) защита информации от несанкционированного доступа и утечек данных;

2) обеспечение целостности, точности и актуальности информации на всех уровнях ее обработки и хранения;

3) гарантированная доступность данных и ИТ-ресурсов для авторизованных пользователей в рабочее время, а также обеспечение бесперебойной работы критически важных систем;

4) снижение рисков утечек информации, атак и угроз, связанных с кибербезопасностью, включая предотвращение взломов, вирусных атак и фишинга;

5) сохранение конфиденциальности данных университета, включая персональные данные студентов, преподавателей и сотрудников, а также научную и коммерческую информацию;

6) проведение регулярных проверок и аудитов системы информационной безопасности для выявления уязвимостей, несоответствий и повышения уровня защиты;

7) обеспечение защиты данных и информационной безопасности в соответствии с международными стандартами ISO/IEC 27001 (системы менеджмента информационной безопасности) и ISO/IEC 27002 (рекомендации по управлению безопасностью информации).

3. Область применения настоящей Политики

3.1. Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Университета. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации Университета, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики. При взаимодействии с третьими лицами обязательно подписание соглашения о неразглашении информации.

3.2. Политика охватывает следующие информационные ресурсы:

1) серверы Университета;

2) сети Университета, включая локальные сети (LAN), Wi-Fi и интернет-ресурсы;

3) программное обеспечение и приложения, используемые для учебной, научной и административной деятельности, включая электронные журналы, образовательные платформы, системы управления данными;

4) персональные устройства, используемые для доступа к корпоративным системам.

4. Принципы информационной безопасности

4.1. Конфиденциальность - информация, находящаяся в распоряжении Университета, должна быть доступна только авторизованным пользователям, а также защищена от утечек и несанкционированного доступа.

4.2. Целостность - необходимо обеспечивать точность и полноту информации, а также предотвращать несанкционированное изменение или уничтожение данных.

4.3. Доступность - информация должна быть доступна для использования уполномоченными лицами в любое время, если это необходимо для учебного процесса, научной работы и административных нужд.

4.4. Аудит и мониторинг - все информационные системы Университета подлежат регулярному аудиту и мониторингу для выявления и предотвращения потенциальных угроз безопасности.

4.1. Общие требования к обеспечению доступа к информации

4.1.1. Запрещается предоставление доступа третьим лицам к конфиденциальной информации Университета за исключением случаев взаимодействия Университета с дистрибьюторами и партнерами, определённых соответствующими юридическими документами (дистрибьюторским договором или иным партнерским соглашением, Договор о неразглашении), включающими в себя обязательные условия защиты данных и ответственность за распространение конфиденциальной информации.

4.1.2. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация Университета.

4.1.3. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят только системные администраторы и специалисты Департамента цифровизации.

4.2. Управление доступом

4.2.1. Идентификация и аутентификация - все пользователи должны проходить процедуру идентификации и аутентификации при доступе к ресурсам Университета (например, использование логинов и паролей, двухфакторная аутентификация).

4.2.2. Права доступа - доступ предоставляется на основе принципа минимальных прав, то есть только тем пользователям, которым необходим доступ к данным для выполнения их обязанностей.

4.2.3. Доступ третьих лиц к информационным системам Университета должен быть обусловлен производственной необходимостью. В связи с этим, доступ к информационным ресурсам Университета должен быть согласован с руководством Университета.

4.2.4. Сотрудники получают право удаленного доступа к информационным ресурсам Университета с учетом их должностных обязанностей. Для предоставления доступа необходимо обосновать потребность и направить запрос на предоставление доступа.

4.2.5. Сотрудникам, которым для работы необходим доступ к рабочим компьютерам Университета, может быть предоставлен удаленный доступ к данным рабочим местам, с которых они могут выполнять работы и иметь доступ к сетевым ресурсам Университета в соответствии с правами в корпоративной информационной системе.

4.2.6. Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам Университета, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Университета и к каким-либо другим сетям, не принадлежащим Университету.

4.2.7. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Университета с внешних сетей, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

4.2.8. Для доступа к сетям и ресурсам Университета могут применяться технические средства ограничения доступа для компьютеров, не соответствующих требованиям по наличию обновлений операционных систем или программного обеспечения, версий вирусных записей антивирусного программного обеспечения или отсутствии защиты.

4.2.9. Запрещается установка, запуск и использование программ для организации удаленного доступа. Программное решения для удаленного подключения сотрудников информационных систем и технической поддержки могут использовать только во внутренней сети Университета. Для возможности удаленной помощи Сотрудники могут использовать возможности контролируемого удаленного подключения или демонстрации экрана, предоставляемые корпоративными коммуникаторами, разрешенными к использованию в Университете.

4.2.10. Отчеты о доступе - все действия с данными должны фиксироваться в журналах доступа.

4.3. Управление инцидентами информационной безопасности

4.3.1. Обнаружение инцидента - сотрудники и студенты обязаны немедленно сообщить о любых подозрительных действиях или инцидентах, связанных с информационной безопасностью.

4.3.2. Процедура реагирования на инцидент - инциденты должны быть зафиксированы, проанализированы и устранены в соответствии с установленной процедурой. В случае серьезных инцидентов, связанных с утечкой данных, следует уведомить пострадавших пользователей.

4.3.3. Восстановление после инцидента - в случае потери данных или нарушений доступности системы, должны быть предприняты меры для восстановления функциональности и данных.

4.3.4. Организация может принять следующие меры для обеспечения информационной безопасности своих систем и данных:

1) технические меры - такие как использование средств защиты от несанкционированного доступа, шифрование данных и резервное копирование;

2) организационные меры - такие как обучение сотрудников информационной безопасности, создание политики информационной безопасности и проведение регулярных проверок системы информационной безопасности;

3) административные меры - такие как управление доступом к системе и данным, а также контроль за использованием информационных систем.

4.4. Шифрование и защита данных

4.4.1. Шифрование данных - конфиденциальная информация должна быть защищена с использованием шифрования как в процессе хранения, так и при передаче по сети.

4.4.2. Защита личных данных - персональная информация студентов, сотрудников и контрагентов должна быть защищена в соответствии с законодательными требованиями.

4.5. Обновления

4.5.1 Обновления программного обеспечения и оборудования являются важным фактором обеспечения информационной безопасности. Обновления могут содержать исправления ошибок, которые могут быть использованы злоумышленниками для получения доступа к системе или информации. Обновления также могут содержать новые функции, которые могут повысить безопасность системы.

4.5.2. Типы обновлений:

1) исправления ошибок - это обновления, которые устраняют ошибки в программном обеспечении или оборудовании;

2) устранение уязвимостей - это обновления, которые устраняют уязвимости в программном обеспечении или оборудовании;

3) добавление новых функций - это обновления, которые добавляют новые функции в программное обеспечение или оборудование.

4.5.2. Важность обновлений:

1) обновления могут повысить безопасность системы, исправляя ошибки и устраняя уязвимости;

2) обновления могут добавить новые функции, которые могут повысить безопасность системы;

3) не установка обновлений может сделать систему уязвимой для атак злоумышленников.

4.5.3. Рекомендации по управлению обновлениями:

1) организация должна иметь политику управления обновлениями, которая определяет порядок и сроки установки обновлений;

2) организация должна обеспечить, чтобы сотрудники знали о важности установки обновлений .

4.6. Программное обеспечение

4.6.1. Все программное обеспечение, установленное на предоставленном Компанией компьютерном оборудовании, является собственностью Университета и должно использоваться исключительно в производственных целях.

4.6.2. 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.

4.6.3. На всех компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации: антивирусное программное обеспечение, персональный межсетевой экран.

4.6.4. Сотрудники Университета не должны:

1) блокировать антивирусное программное обеспечение;

2) устанавливать другое антивирусное программное обеспечение;

3) изменять настройки и конфигурацию антивирусного программного обеспечения.

4.6.5. На корпоративные системы применяются ограничительные меры по возможности установки программного обеспечения. Для установки необходимого программного обеспечения на корпоративные устройства, Сотрудники должны обратиться в Департамент цифровизации на установку необходимого программного обеспечения. Необходимость установка должна быть обоснована, должна быть обеспечена лицензиями, либо программное обеспечение должно быть свободного для использования, иметь бесплатную лицензию.

4.7. Сообщение об инцидентах информационной безопасности, реагирование и отчетность

4.7.1. Все пользователи должны быть осведомлены непосредственным руководителем о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны

пытаться использовать ставшие им известными слабые стороны системы безопасности.

4.7.2. В случае кражи компьютера следует незамедлительно сообщить об инциденте непосредственному руководителю.

4.7.3. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

1) проинформировать специалистов службы поддержки;

2) не пользоваться и не выключать зараженный компьютер;

3) не подсоединять этот компьютер к компьютерной сети Университета до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами службы поддержки.

4.8. Управление сетью

4.8.1. Сотрудникам Университета запрещается:

1) нарушать информационную безопасность и работу сети Университета; сканировать порты или систему безопасности;

2) контролировать работу сети с перехватом данных;

3) получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

4) использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

5) передавать информацию о сотрудниках или списки сотрудников Университета посторонним лицам;

6) создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

5. Требования к информационным системам и сетям

5.1. Минимальные требования

5.1.2. Все информационные системы и сети Университета должны соответствовать минимальным стандартам безопасности, которые включают:

1) регулярные обновления программного обеспечения;

2) установка антивирусных программ и межсетевых экранов;

3) шифрование данных при передаче по сети.

5.2. Защита сетевых соединений

5.2.1. Все данные, передаваемые по сети, должны быть защищены с использованием современных средств шифрования и защищенных протоколов (например, HTTPS, SSL/TLS).

6. Управление рисками и инцидентами

6.1. Управление рисками

6.1.1. В Университете проводится регулярная оценка рисков информационной безопасности, включая угрозы утечек данных, внешние атаки и технические сбои. Для каждого типа угроз разрабатываются меры по минимизации рисков.

6.2. Реагирование на инциденты

6.2.1. В случае возникновения инцидента информационной безопасности (например, утечка данных, взлом системы) должны быть предприняты немедленные меры:

1) локализация инцидента;
2) анализ причин и последствий;
3) восстановление нормальной работы системы.

6.3. Оценка рисков и планирование на случай чрезвычайных ситуаций

6.3.1. Чрезвычайными ситуациями считаются события, которые могут привести к значительному ущербу для инфраструктуры, информации или людей в университете. Включает кибератаки, природные катастрофы, террористические угрозы, а также события, которые могут нарушить нормальный процесс образовательной и научной деятельности.

6.3.2. Регулярная оценка рисков информационной безопасности поможет выявить потенциальные угрозы и уязвимости.

6.3.3. Университет разрабатывает и внедряет план восстановления после чрезвычайных ситуаций (Disaster Recovery Plan, DRP), чтобы минимизировать последствия инцидентов безопасности.

6.3.4. Этот план направлен на восстановление всех ключевых систем, данных и сервисов после различных инцидентов, таких как кибератаки, природные катастрофы или технические сбои.

6.3.5. Основные элементы плана восстановления:

1) определение критичных систем и данных: Выделение наиболее важных для работы университета сервисов, таких как системы управления обучением (LMS), базы данных студентов и сотрудников, финансовые и административные системы;

2) резервирование данных и инфраструктуры: Регулярное создание резервных копий данных, поддержка резервных серверов и инфраструктуры, готовых к быстрому восстановлению;

3) процедуры восстановления: Детализированные инструкции по восстановлению информационных систем в случае чрезвычайной ситуации, включая технические шаги, сроки восстановления и приоритеты восстановления;

4) распределение ответственности: Определение ответственных за действия в случае чрезвычайной ситуации, включая Департамента цифровизации, службу безопасности, администрацию и внешних подрядчиков.

6.3.6. План восстановления должен обеспечивать как оперативное восстановление (в течение первых часов или дней после инцидента), так и долгосрочную восстановительную работу, направленную на минимизацию воздействия инцидента на учебный процесс и репутацию университета.

6.3.7. План восстановления подвергается регулярному тестированию, включая симуляции различных типов инцидентов для проверки эффективности восстановления. Результаты тестов и реальных инцидентов используются для постоянного улучшения плана.

7. Организационная структура

7.1. Ответственные лица

7.1.1. Ответственность за организацию и реализацию политики информационной безопасности в Университете возлагается на Департамент цифровизации, который несет полную ответственность за защиту всех информационных систем и данных учебного заведения.

7.1.2. Степень ответственности за нарушение требований локальных нормативных актов в области информационной безопасности определяется в каждом конкретном случае и может включать как дисциплинарные меры, так и юридическую ответственность в зависимости от характера и последствий нарушения.

7.1.3. Руководители структурных подразделений несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях. Они обязаны незамедлительно сообщать в Департамент цифровизации о всех инцидентах, связанных с нарушениями требований информационной безопасности, а также принимать меры для минимизации последствий таких инцидентов и предотвращения их повторения в будущем.

7.2. Обязанности ответственных лиц

7.2.1. Департамент цифровизации выполняет следующие обязанности:

1) разработка и внедрение политики информационной безопасности;

2) обеспечение защиты информационных систем, сетей и данных;

3) оценка рисков и проведение мероприятий по снижению угроз безопасности;

4) осуществление контроля за выполнением требований по информационной безопасности;

5) обучение сотрудников и студентов основам безопасного обращения с информационными системами;

6) координация действий в случае возникновения инцидентов информационной безопасности.

7.2.2. Руководитель Департамента цифровизации назначается ответственным за информационную безопасность Университета и непосредственно курирует все процессы, связанные с этим вопросом.

8. Заключение

8.1. Политика информационной безопасности Университета является обязательной для выполнения всеми сотрудниками, студентами и контрагентами, имеющими доступ к информационным системам Университета. Соблюдение всех ее требований направлено на создание безопасной среды для учебного процесса, научных исследований и работы университетских систем, а также на защиту интересов всех участников образовательной деятельности.

8.2. Политика информационной безопасности университета будет регулярно пересматриваться и обновляться в ответ на изменения в законодательстве, технологические новшества, а также в случае выявления новых угроз. Обновления также будут проводиться на основе анализа инцидентов безопасности, рекомендаций от внутренних и внешних аудиторов.

8.3. Политика будет учитывать требования национальных и международных стандартов, а также обеспечивать соответствие действующему законодательству в области защиты данных и кибербезопасности.

9. Лист регистрации изменений

№ п/п	Номера листов			Основание для внесения изменений	Подпись	Ф.И.О.	Дата	Дата введения изменения
	заменённых	новых	аннулированных					