Государственное казначейское учреждение здравоохранения Республики Башкортостан
«Медицинский информационно-аналитический центр»

УТВЕРЖДАЮ

И.о. директора ГКУЗ РБ МИАЦ

_____ А.З. Муртазин
«20» апреля 2022 года

ПАРОЛЬНАЯ ПОЛИТИКА

в отношении Государственной информационной системы
«Республиканская медицинская информационно-аналитическая система Республики Башкортостан»
(ГИС «РМИАС РБ»)

Уфа 2022

Оглавление

1. Общие сведения

1.1 Настоящая Политика устанавливает требования к порядку выбора, хранения, использования, периодичности смены и другим вопросам, связанным с применением механизмов парольной аутентификации в ГИС «ГИС «РМИАС РБ»».

1.2 Требования настоящей Политики распространяются на всех пользователей ГИС «ГИС «РМИАС РБ»», а также всех прочих лиц (подрядчики, аудиторы и т.п.) в установленном порядке получивших право на доступ к ресурсам ГИС «РМИАС РБ» в соответствии с функциональными обязанностями.

2. Термины и определения

Термин	Определение
Информационная система	- овокупность программного обеспечения и технических средств, спользуемых для хранения, обработки и передачи информации, с елью решения бизнес-задач подразделений Компании. В Компании спользуются различные типы информационных систем для ешения производственных, управленческих, учетных и других изнес-задач.
ГИС «РМИАС РБ»	- государственная информационная система Республики Башкортостан, состоящая из комплекса программных и технических средств, баз данных, обеспечивающих информационно-технологическую поддержку функционирования системы здравоохранения Республики Башкортостан, и предназначенную для выполнения в Республике Башкортостан функций регионального фрагмента Единой государственной информационной системы в сфере здравоохранения.
Пользователи ГИС «РМИАС РБ»	- работники медицинских организаций (штатные, временные, работающие по контракту и т.п.), администраторы ГИС «РМИАС РБ», а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в ГИС «РМИАС РБ» в установленном порядке.
Пароль пользователя	- секретная (известная только данному пользователю) последовательность символов, используемая пользователем для подтверждения своей подлинности (аутентификации) при входе в систему (сеть), а также (в некоторых случаях) для получения доступа к информационным ресурсам.
Учетная запись пользователя	- хранимая в компьютерной системе совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа к данным и настройкам. Учетная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п.
Аутентификация	- проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.
Несанкционированный доступ	- доступ к информации, нарушающий установленные правила разграничения доступа.

3. Основные положения

3.1 Пароли для доступа к ГИС «РМИАС РБ» предоставляются пользователям администратором при регистрации этих сотрудников в качестве пользователей ГИС «РМИАС РБ». При получении первоначального пароля от администратора, пользователь обязан произвести смену этого пароля при первом входе в ГИС «РМИАС РБ». В дальнейшем пользователь должен осуществлять смену своих паролей самостоятельно в соответствии с требованиями настоящей Политики.

3.2 Пользователи ГИС «РМИАС РБ» должны производить смену своих паролей не реже, чем раз в три месяца.

3.3 Пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.

3.4 С целью предотвращения несанкционированного доступа к рабочим местам пользователей, а также к ресурсам ГИС «РМИАС РБ» с использованием чужих учетных записей (имен пользователей), пользователи обязаны блокировать экраны своих компьютеров в случае оставления ими своего рабочего места нажатием на компьютерной клавиатуре набора клавиш Ctrl+Alt+Del и далее - кнопки «Блокировать компьютер».

3.5 Все выбираемые пользователями пароли должны отвечать приведенным ниже требованиям:

- Содержать не менее 8 символов.

- Содержать символы, набранные в разных регистрах (a-z, A-Z)

- Помимо букв, содержать также цифры, знаки препинания и/или специальные символы (0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Не являться словом из словаря, сленга, диалекта, жаргона и т.п.

- Не являться персональной информацией (имена членов семьи, адреса, телефоны, даты рождения и т.п.)

3.6 Пользователи могут выбрать легко запоминающиеся пароли, которые в то же время являются трудно угадываемыми для других лиц, если будет выполнено хотя бы одно из следующих условий:

- Несколько слов написаны слитно (такие пароли известны под названием «passphrases»);

- Набор слова на русском языке на английской раскладке клавиатуры

- Намеренно неправильное написание слова (но не обычная в данном слове орфографическая ошибка).

4. Обеспечение конфиденциальности паролей

4.1 Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

4.2 Любые действия, выполненные в информационной системе (просмотр, внесение сведений, удаление, исправления…) под определенной учетной записью, считаются выполненными обладателем этой учетной записи, даже если они были выполнены третьим лицом, получившим санкционированный или несанкционированный доступ к ней, если не было установлено лицо осуществившее неправомерный доступ к информации.

4.3 Запрещается:

- Сообщать свой пароль кому-либо, включая коллег, руководителей и специалистов службы технической поддержки, по телефону, по электронной почте или какими-либо иными средствами.

- Хранить пароли в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к

ним доступ. Например, ни в каких приложениях пользователи не должны выбирать такую опцию конфигурации, как автоматическое сохранение пароля.

- Записывать пароли и оставлять эти записи в местах, где к ним могут получить доступ неуполномоченные лица.
- Произносить свой пароль вслух.
- Использовать общие пароли совместно с другими пользователями.

4.4 Примечания:

1. Если кто-либо требует от Вас раскрытия пароля, сошлитесь на настоящую Политику или предложите обратиться за разъяснениями в Отдел информационной безопасности ГКУЗ РБ МИАЦ по телефону 8(347)291-28-32.

2. Пароль должен быть немедленно изменен, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого пользователя.

3. Системным администраторам для выполнения ими своих служебных обязанностей, ни при каких обстоятельствах, не требуется знание паролей пользователей. Для этого у них есть все необходимые полномочия в ИС. В случае необходимости, они произведут смену пароля пользователя и сообщат ему об этом.

5. Контроль

5.1 Общий контроль выполнения требований настоящей Политики осуществляется сотрудниками отдела информационной безопасности ГКУЗ РБ МИАЦ. С целью проверки надежности используемых паролей по согласованию с системными администраторами ими периодически могут осуществляться тестовые «взломы» паролей пользователей. Системные администраторы имеют право принимать участие в проведении подобных проверок. По указанию сотрудников отдела информационной безопасности ГКУЗ РБ МИАЦ, пользователи должны производить смену паролей, не удовлетворяющих критериям надежности, устанавливаемым настоящей Политикой.

5.2 Системные администраторы там, где это возможно, должны настраивать в операционных системах и приложениях следующие параметры парольной политики:

- Минимальная длина пароля – 8 символов;
- Пароль должен отвечать требованиям сложности;
- Максимальный срок действия пароля – 90 дней;
- Минимальный срок действия пароля – 1 день;
- Не повторяемость паролей (хранить 5 предыдущих);
- Использование шифрования при хранении паролей;
- Автоматическая блокировка пользовательских учетных записей после 5 неудачных попыток введения пароля. (Последующая разблокировка пользовательского пароля может производиться только системным администратором).

5.3 Системные администраторы также осуществляют настройку на рабочих местах пользователей автоматического блокирования экранов через 15 минут неактивности.

6. Ответственность

6.1 На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования настоящей Политики, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы за неоднократное грубое нарушение правил работы с ГИС «РМИАС РБ».