ПРИЛОЖЕНИЕ 1
к приказу государственного автономного
учреждения Республики Коми
«Центр информационных технологий»
от _____ № _____

ПОЛИТИКА
информационной безопасности «Парольная политика для пользователей, не имеющих административные полномочия»

1. Используемые сокращения

АРМ	автоматизированное рабочее место
ГАУ РК «ЦИТ»	государственное автономное учреждение Республики Коми «Центр информационных технологий
ГИС	государственная информационная система Республики Коми
ЗОКИИ	значимые объекты критической информационной инфраструктуры органов государственной власти Республики Коми и государственных учреждений Республики Коми
ИС	информационная система
ОС	операционная система
ПО	программное обеспечение
СЗИ	средство защиты информации

2. Общие положения

Настоящая политика информационной безопасности «Парольная политика для пользователей, не имеющих административные полномочия» (далее – Политика) определяет обязательные требования к минимальным характеристикам и защите паролей учетных записей типа «пользователь» домена RK.local, а также паролей, используемых для аутентификации в ГИС, ЗОКИИ, иных ИС, находящихся на обслуживании ГАУ РК «ЦИТ».

Учетные записи разделены на следующие виды:

– пользовательские – учетные записи пользователей, не имеющих административных полномочий;

– общие – учетные записи, предназначенные для использования несколькими лицами, например, учетные записи отделов, организаций, общих почтовых ящиков, календарей.

3. Требования к характеристикам паролей

3.1. Требования к характеристикам паролей общих и пользовательских учетных записей приведены в таблице 1.

Таблица 1

Виды учетной записи	Количество символов	Комбинация символов	Примеры
Общие Пользовательские	Не менее 8	Не менее 3-х групп символов из предложенных: • строчные буквы, • прописные буквы, • цифры, • специальные символы	Bt73Mq62 S9cap$D 73YTw?!zG

3.2. Пароли не должны подпадать под характеристики слабых паролей:

– состоящие из повторяющегося символа или группы символов (*например: 1111qqqq, 123123123, passpass*);

– состоящие из символов, расположенных на клавиатуре подряд (*например, qwerty123*);

– используемые для авторизации в социальных сетях, почтовых сервисах, на форумах или на домашних персональных компьютерах;

– слова St@ndart, P@ssw0rd, Qwerty123 а также их модификации;

– никнеймы (псевдонимы, используемые пользователем в Интернете), имена (собственное имя, имена родственников);

– клички домашних животных;

– романтические отсылки (нынешние или прошлые);

– биографическая информация (дата рождения);

– имя учетной записи пользователя или какая-либо его часть.

3.3. При отсутствии официальной возможности в программном продукте установить требуемый пароль без закупки дополнительных лицензий (расширений) устанавливаются максимально близкие требования из возможных к установке.

3.4. Запрещается использовать один и тот же пароль для разных учетных записей и на разных устройствах (например, для входа в ГИС использовать такой же пароль как для входа в ОС).

3.5. Пароли, используемые для аутентификации в ГИС и ЗОКИИ, должны отвечать требованиям настоящей Политики, если иное не установлено в проектной и рабочей документации на соответствующую ГИС или ЗОКИИ.

3.6. В ОС, ГИС, ЗОКИИ, иных ИС максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки 10 попыток за 20 минут. В случае достижения установленного максимального количества неуспешных попыток аутентификации должна быть осуществлена автоматическая блокировка учетной записи или IP-адреса атакующего на 30 минут.

4. Требования и рекомендации к передаче, генерации, смене и хранению паролей

4.1. Передачу паролей разрешается осуществлять только в случае использования общих учетных записей для исполнения должностных обязанностей.

4.2. Передачу паролей в случае, указанном в пункте 4.1 настоящей Политики, необходимо осуществлять посредством Системы передачи паролей ГАУ РК «ЦИТ» (сайт pwd.rkomi.ru) или по защищенным каналам связи (например, с помощью VPN соединения, образуемого сертифицированными средствами защиты информации), либо в защищенном виде (например, с помощью зашифрованного архива с одноразовым паролем (ссылка на одноразовый пароль формируется на сайте pwd.rkomi.ru и направляется отдельно от архива).

4.3. Для генерации паролей запрещается использовать внешние (не размещенные локально на АРМ) сервисы и сайты.

4.4. Смена пароля должна проводиться не реже одного раза в 90 дней.

4.5. После получения пароля от других лиц (например, при создании учетных записей) необходимо, при наличии в программном продукте функционала смены пароля, сменить его в соответствии с требованиями Политики в течение 1 рабочего дня.

4.6. В случае прекращения полномочий (увольнение и т.п.) работника должна производиться смена его паролей или блокировка учетных записей в течение 1 рабочего дня, при большом количестве учетных записей – в течение 5 рабочих дней.

4.7. Хранение паролей на бумажном носителе допускается только в личном сейфе, запирающемся шкафу.

4.8. Хранение паролей пользовательских и общих учетных записей на АРМ и общих сетевых папках запрещается.

4.9. Необходимо соблюдать правила безопасной работы с электронной почтой (https://security.rkomi.ru/node/3).

4.10. Информацию о попытках получения или требования пароля третьими лицами работникам необходимо сообщать непосредственному руководителю.

5. Ответственность

5.1. За нарушение требований настоящей Политики предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.