Данный регламент определяет политики доступа и безопасности для базы данных Ceramic, управляемой через SQL Server Management Studio (SSMS) 20. Он включает в себя роли пользователей, политику резервного копирования.

Роли пользователей

Администратор (Administrator):

* + Описание: Обладает полным контролем над базой данных.
  + Права: Все права (db\_owner).
  + Применение: Для пользователей, ответственных за обслуживание, настройку и поддержку базы данных (например, DBA).

Редактор (Editor):

* + Описание: Может добавлять, изменять и удалять данные в таблицах.
* db\_datawriter: Разрешает вставку, обновление и удаление данных во всех таблицах.
* db\_datareader: Разрешает чтение данных из всех таблиц и представлений.
* Применение: Для пользователей, которые непосредственно работают с данными и нуждаются в возможности их изменения (например, инженеры по контролю качества, операторы ввода данных).

Читатель (Reader):

* Описание: Может только читать данные из таблиц и представлений.
* db\_datareader: Разрешает чтение данных из всех таблиц и представлений.
* Применение: Для пользователей, которым требуется доступ к данным только для просмотра и анализа (например, менеджеры, аналитики).

Политика резервного копирования:

Регулярное резервное копирование - критически важная часть стратегии защиты данных.

Типы резервных копий:

* + Полная резервная копия: Создает полную копию всей базы данных. Рекомендуется выполнять как минимум раз в неделю.
  + Разностная резервная копия: Копирует только изменения, внесенные с момента последней полной резервной копии. Рекомендуется выполнять ежедневно.
  + Резервная копия журнала транзакций: Копирует журнал транзакций, что позволяет восстановить базу данных до определенного момента времени. Рекомендуется выполнять каждые несколько часов (в зависимости от интенсивности транзакций).

Схема резервного копирования:

1. Полная резервная копия: Каждое воскресенье в 2:00 ночи.
2. Разностная резервная копия: Ежедневно в 2:00 ночи (кроме воскресенья).
3. Резервные копии журнала транзакций: Каждые 2 часа в течение рабочего дня (например, с 8:00 до 18:00).
4. Место хранения резервных копий: Хранить резервные копии в безопасном месте, отличном от сервера базы данных. Рассмотрите возможность использования облачного хранилища для дополнительной защиты.
5. Проверка резервных копий: Регулярно проверяйте работоспособность резервных копий, выполняя тестовое восстановление на тестовом сервере.