**1. Область применения**

Данная политика определяет меры безопасности для защиты базы данных "Логистическая система", включая доступ к данным, их хранение, передачу и резервное копирование.

**2. Управление доступом**

* Доступ к базе данных предоставляется только авторизованным пользователям и приложениям.
* Используется модель наименьших привилегий: каждому пользователю или роли предоставляются только те права, которые необходимы для выполнения его функций (например, только чтение, или чтение/запись только в определенные таблицы).
* Права доступа регулярно пересматриваются.
* Несанкционированные попытки доступа отслеживаются.

**3. Аутентификация**

* Пользователи должны проходить аутентификацию (подтверждать свою личность) при каждом подключении к базе данных.
* Используются надежные методы аутентификации (например, пароли, сертификаты).
* Пользователям рекомендуется использовать надежные пароли и регулярно их менять.

**4. Защита данных**

* **Конфиденциальность:**
  + Для защиты данных при передаче по сети рекомендуется использовать шифрование (SSL/TLS) при подключении.
  + На уровне операционной системы могут применяться меры по шифрованию дисков, где хранятся данные базы данных.
* **Целостность:**
  + Структура базы данных с использованием первичных и внешних ключей обеспечивает целостность данных и предотвращает некорректные или противоречивые записи.
  + Регулярно проводятся проверки целостности данных.
* **Доступность:**
  + Принимаются меры для обеспечения стабильной работы сервера базы данных.

**5. Мониторинг и аудит**

* Ведется журнал аудита, фиксирующий подключения, попытки входа в систему, а также критические операции с данными (изменение, удаление).
* Проводится регулярный мониторинг активности базы данных для выявления подозрительного поведения.

**6. Резервное копирование и восстановление**

* Регулярно выполняется полное и/или инкрементальное резервное копирование базы данных.
* Копии хранятся на надежных носителях, в том числе вне серверной площадки, чтобы защититься от физических угроз.
* Периодически проводится тестирование процедуры восстановления данных из резервных копий для проверки их работоспособности.
* План аварийного восстановления (Disaster Recovery Plan) документирован и поддерживается в актуальном состоянии.

**7. Реагирование на инциденты безопасности**

* Определены процедуры на случай возникновения инцидентов безопасности (например, несанкционированный доступ, утечка данных).
* В случае обнаружения инцидента необходимо немедленно сообщить ответственному специалисту: [Контакты или процедура сообщения].

**8. Пересмотр Политики**

Данная Политика безопасности подлежит периодическому пересмотру и актуализации (например, раз в год или при существенных изменениях в инфраструктуре или угрозах).