Security Architecture

1. **Загальна архітектура безпеки**
   - *Фізична Безпека*
     - Контроль доступу до фізичного оточення:
       Забезпечити обмежений доступ до приміщень, де зберігається апаратна частина AREG та де здійснюється розробка контенту.
   - *Апаратна Безпека*
     - Контроль доступу до AR-окулярів:
       Використовувати механізми аутентифікації для забезпечення, що тільки власник AR-окулярів має доступ до функцій системи.
     - Шифрування даних на AR-окулярах:
       Забезпечити шифрування даних, зокрема відомостей про користувача та результатів взаємодії, щоб запобігти несанкціонованому доступу.
   - *Мережева Безпека*
     - Захист від атак на мережевому рівні:
       Використовувати заходи безпеки, такі як фаєрволи та системи виявлення вторгнень для захисту мережевого з'єднання між AR-окулярами та іншими компонентами системи.
     - Шифрування мережевого трафіку:
       Застосовувати шифрування для всього мережевого трафіку, що передається між AR-окулярами та іншими компонентами системи.
   - *Системи Аутентифікації та Авторизації*
     - Двофакторна аутентифікація користувачів:
       Забезпечити можливість використання двофакторної аутентифікації для підвищення рівня безпеки облікових записів користувачів.
     - Керування правами доступу:
       Реалізувати систему керування правами доступу для кожного користувача та системного адміністратора.
2. **Операційна Безпека**
   - *Захист Апаратної Платформи*
     - Регулярні оновлення безпеки апаратних компонентів:
       Забезпечити систему автоматичних оновлень для підтримки безпеки апаратних компонентів AR-окулярів.
   - *Захист Операційної Системи*
     - Оновлення та патчі для операційної системи:
       Здійснювати регулярні оновлення та встановлення патчів для операційної системи AR-окулярів.
3. **Захист Даних**

- *Шифрування Даних*
  - Шифрування даних на рівні баз даних:
    Забезпечити шифрування чутливих даних на рівні баз даних для захисту від несанкціонованого доступу.
  - Шифрування даних під час передачі:
    Використовувати шифрування для захисту даних, що передаються між AR-окулярами та серверами.

4. **Захист Програмного Забезпечення**
   - *Тестування Безпеки*
     - Регулярне тестування на проникнення:
       Проводити регулярні тести на проникнення для виявлення та виправлення потенційних вразливостей програмного забезпечення.
   - *Контроль Змін*
     - Моніторинг змін у програмному забезпеченні:
       Забезпечити систему моніторингу для виявлення та контролю змін, внесених до програмного забезпечення.
5. **Аудит та Моніторинг**
   - *Журналювання Подій*
     - Реалізація журналювання подій:
       Забезпечити систему журналювання подій для відстеження дій користувачів та системних подій.
   - *Моніторинг Доступу*
     - Система моніторингу доступу:
       Встановити систему моніторингу для виявлення надто активного чи невірного використання системи та коригування відповідно.
6. **Реагування на Інциденти**
   - *План Реагування на Інциденти*
     - Розробка плану реагування на інциденти:
       Створення детального плану дій у випадку виявлення безпекового інциденту.
   - *Команда Реагування на Інциденти*
     - Тренування команди реагування на інциденти:
       Проводження регулярних тренувань для команди реагування на інциденти з метою підвищення ефективності в разі виникнення проблем