Findings to be added to Circuitil for ensure compliance with Play Store policies.

- Content Moderation (Image & Text)
- Provide an in-app mechanism for user feedback.
- Age Verification.
- Auto-ban & Account Monitoring.
- Provide a Child Safety Point of Contact (Add this information to your **Terms of Service** and **Privacy Policy**).
- **Update the Terms of Use & Community Guidelines**
  - Clearly define objectionable content (e.g., nudity, hate speech, harassment).
  - Prohibit illegal content and child endangerment.
- Change the social media icons for avoiding copyrights.
- Use Check box for accepting terms and conditions.
- Requesting permission before accessing camera, contacts, or location.
- If you collect sensitive user data, provide a clear consent prompt.
- Create a Consent Dialog.
- **Privacy Policy Must Include :**
  - Your **developer/company name & contact** details.
  - **What data you collect** (e.g., user profile, chat messages, images).
  - **Why you collect it** (e.g., improve influencer-brand collaboration).
  - **Who has access to it** (e.g., Firebase, backend server, no third parties).
  - **How it's stored and protected** (e.g., encryption, secure servers).
  - **Data retention & deletion policies.**
  - **A section titled "Privacy Policy".**
- When users delete their account, **permanently delete all their data** (not just deactivate).
- **Only request necessary permissions**
  - If your app requests sensitive permissions (like location, camera, microphone, contacts, or storage),
  - they must be directly related to features you provide.
  - You must explain why you need these permissions through in-app disclosures when requesting them.
- **Update your privacy policy and Data Safety section**
  - If your app collects personal data (name, email, location, photos, etc.), your privacy policy must clearly disclose it.
  - The privacy policy must explain how you collect, use, share, and store this data.
- Review your app's permissions in AndroidManifest.xml and **remove any unnecessary ones.**
- Remove READ_EXTERNAL_STORAGE, READ_MEDIA_IMAGES, or READ_MEDIA_VIDEO from AndroidManifest.xml if they are currently included.
- **Privacy Policy Updates for permissions**

  Since you're not using MANAGE_EXTERNAL_STORAGE, only include:
  - Camera access statement
  - Gallery access statement
  - Example:

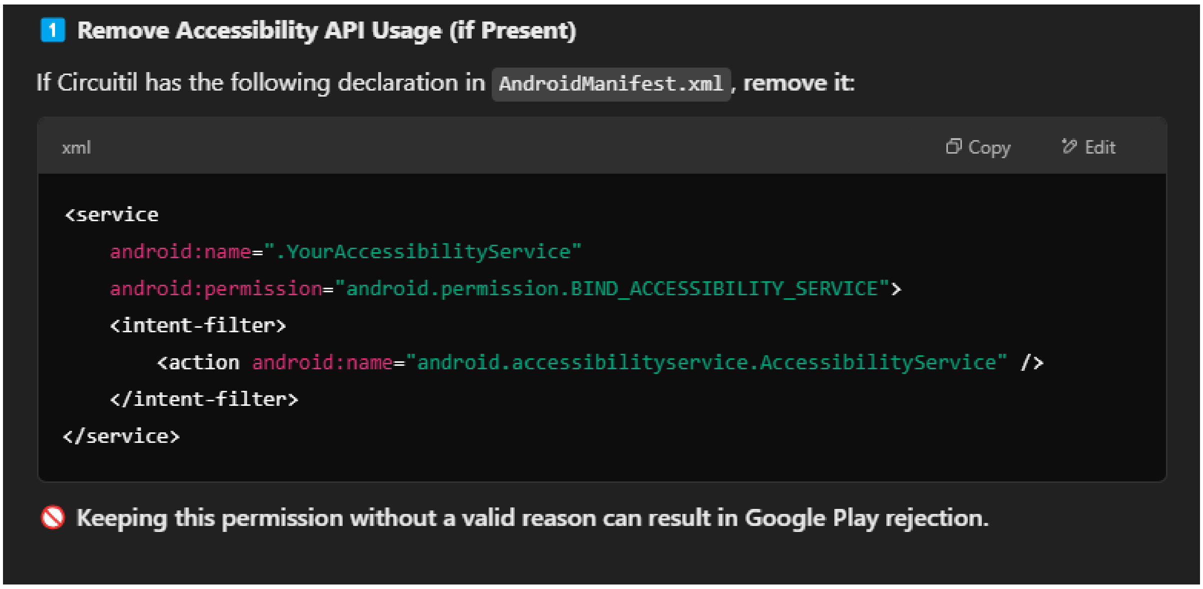
    "Our app requires access to the camera to capture photos and the gallery to upload existing images. We do not store or share your photos without your permission."
- Do not use MANAGE_EXTERNAL_STORAGE (not needed for photos/videos upload).
- **Privacy Policy Updates for permissions**

  Your privacy policy should clearly state:

  - The app only accesses photos/videos when the user selects them.
  - It does not store or share photos without user permission.
  - It does not require broad storage access.
  - Example:

    "Circuitil requires access to the camera to capture photos and access to the gallery for selecting images. The selected images are uploaded to our secure servers and are not shared with third parties. We do not access or store media files without user permission."

- QUERY_ALL_PACKAGES in AndroidManifest.xml, remove it:
- Ensure your **Privacy Policy states** that Circuitil does not collect, store, or share installed app data.
  - Example Update:
    "Circuitil does not access, store, or share a list of installed apps on the user's device. The app only interacts with the device's camera and gallery for image uploads."
-



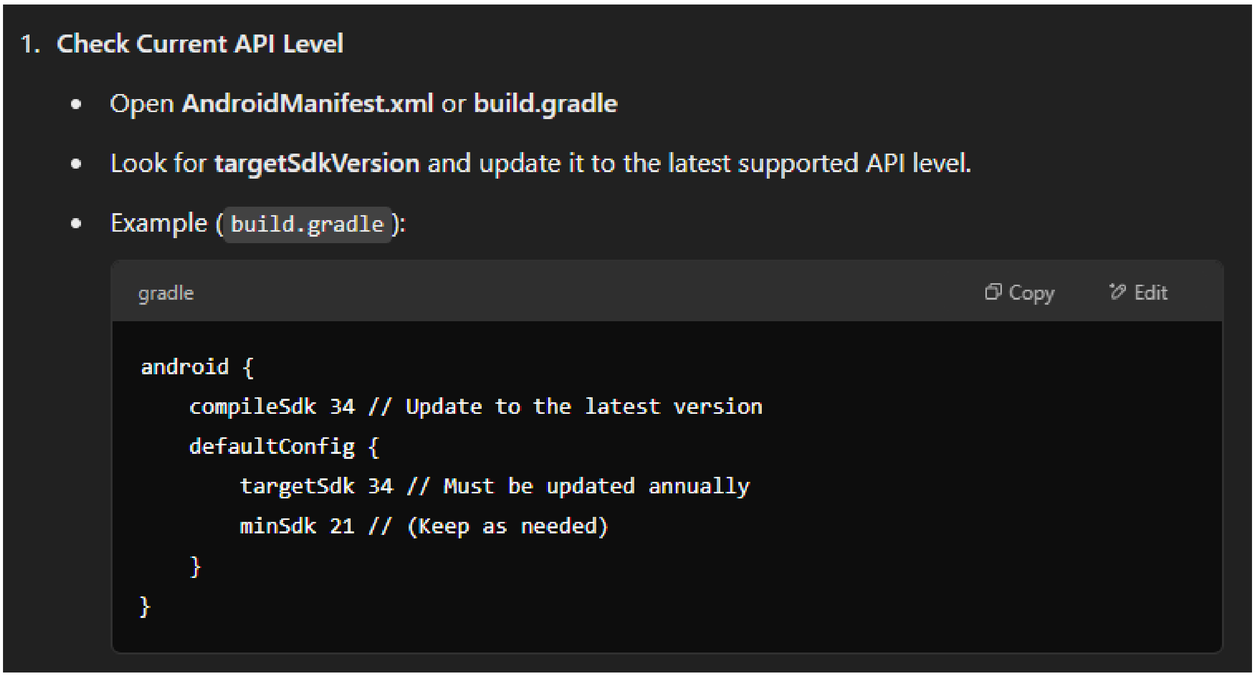
1️⃣ Remove Accessibility API Usage (if Present)

If Circuitil has the following declaration in `AndroidManifest.xml`, **remove it:**

```xml
<service
    android:name=".YourAccessibilityService"
    android:permission="android.permission.BIND_ACCESSIBILITY_SERVICE">
    <intent-filter>
        <action android:name="android.accessibilityservice.AccessibilityService" />
    </intent-filter>
</service>
```

🚫 **Keeping this permission without a valid reason can result in Google Play rejection.**

- <u>**Accessibility Services in privacy policy**</u>
  "Circuitil does not use the Android Accessibility API. We do not collect or modify user interactions, control device settings, or perform automated actions using Accessibility Services."
- <u>**Privacy Policy Changes Needed**</u>
  Ensure Circuitil's Privacy Policy Includes:
  - A statement confirming no unauthorized data access, interference, or security bypasses.
  - Details on how APIs and third-party services comply with their terms.
  - Information on WebView security (if applicable).
  - Clarification that Circuitil follows Google Play's update mechanism and does not install unauthorized apps.
  - Review the privacy policy and update sections related to data security, WebView usage, and third-party API compliance.
  - Check the app code to ensure there's no dynamic executable code loading from external sources.
  - We do not perform background data transfers without user interaction.
- If Circuitil currently declares FOREGROUND_SERVICE_NOTIFICATION permission, **it can be removed.**
- <u>**Privacy Policy Update (If Necessary)**</u>
  If Circuitil already mentions how FCM handles notifications and data, no updates are needed.
  If not, add a statement like:
  "Circuitil uses Firebase Cloud Messaging (FCM) to deliver notifications to users. These notifications are handled by the Firebase service and do not require continuous background activity."
- **Manifest Check for Compliance**
  Ensure the app does not declare any unnecessary foreground service permissions (FOREGROUND_SERVICE, FOREGROUND_SERVICE_NOTIFICATION).

- 

  1. **Check Current API Level**
     - Open **AndroidManifest.xml** or **build.gradle**
     - Look for **targetSdkVersion** and update it to the latest supported API level.
     - Example (`build.gradle`):

```gradle
android {
    compileSdk 34 // Update to the latest version
    defaultConfig {
        targetSdk 34 // Must be updated annually
        minSdk 21 // (Keep as needed)
    }
}
```

- Ensure that your use of an SDK does not violate policy requirements.
- Ensure the app description accurately explains all its features (collaborations, chat, notifications, profile visits, etc.).
- Mention any background processes (e.g., push notifications, API data fetching).
- Include a clear settings page explaining available permissions and their purpose.
- **Privacy Policy**
  - Mention any background data usage, push notifications, and storage access in the privacy policy.
  - If the app modifies system settings (e.g., notifications, storage), clearly disclose this in the policy.
  - **Ensuring Transparent and Secure App Functionality.**
    - Circuitil does not download or install any external apps or files without explicit user consent, does not trigger hidden installations, ensures all downloads are user-initiated, and verifies that third-party SDKs comply with these principles.
- **Privacy Policy Update (if needed):**
  If Circuitil uses notifications, the privacy policy should clarify:
  - The purpose of notifications (e.g., chat alerts, collaboration updates).
  - That the app does not send misleading or system-mimicking notifications.
  - Users have control over notification preferences.
  - Clearly state that Circuitil is not designed for children and is intended for adults and professionals in brand-influencer collaborations.
- Ensure that all submitted data, especially in the Target audience and content section, is truthful to prevent app suspension.